

Ethernet Switch

CLI Reference Guide

Default Login Details

IP Address	http://192.168.0.1 (Out-of-band MGMT port)
	http://192.168.1.1 (In-band ports)
User Name	admin
Password	1234

Firmware Version 3.79, 3.80, 3.90
and 4.00
Edition 3, 11/2011

www.zyxel.com

The logo for ZyXEL, featuring the company name in a bold, blue, sans-serif font. The 'Z' and 'Y' are stylized with a slight slant.

About This CLI Reference Guide

Intended Audience

This manual is intended for people who want to configure ZyXEL Switches via 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 version 3.79, 3.80, 3.90 and 4.00 at the time of writing.



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

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

How To Use This Guide

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

Document Conventions

Warnings and Notes

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



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



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

Syntax Conventions

This manual follows these general conventions:

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

Command descriptions follow these conventions:

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

The following is an example of a required field within an optional field: `snmp-server [contact <system contact>]`, the `contact` field is optional. However, if you use `contact`, then you must provide the `system contact` information.

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

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

Command summary tables are organized as follows:

Table 1 Example: Command Summary Table

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

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

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

- If a command is not indented, you run it in the enable or config mode. See [Chapter 2 on page 17](#) for more information on command modes.
- If a command is indented, you run it in a sub-command mode.

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

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

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

The **P** column identifies the privilege level of the command. If you don't have a high enough privilege level you may not be able to view or execute some of the commands. See [Chapter 2 on page 17](#) for more information on privilege levels.

Icons Used in Figures

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

Switch 	Computer 	Notebook computer 
Server 	DSLAM 	Firewall 
Telephone 	Switch 	Router 

Contents Overview

Introduction	11
How to Access and Use the CLI	13
Privilege Level and Command Mode	17
Initial Setup	23
Reference A-G	27
AAA Commands	29
ARP Commands	31
ARP Inspection Commands	33
ARP Learning Commands	39
Bandwidth Commands	41
Broadcast Storm Commands	45
CFM Commands	49
Classifier Commands	59
Cluster Commands	63
Date and Time Commands	67
DHCP Commands	71
DHCP Snooping & DHCP VLAN Commands	75
DiffServ Commands	79
Display Commands	81
DVMRP Commands	83
Error Disable and Recovery Commands	85
Ethernet OAM Commands	89
External Alarm Commands	95
GARP Commands	97
GVRP Commands	99
Reference H-M	101
HTTPS Server Commands	103
IEEE 802.1x Authentication Commands	107
IGMP and Multicasting Commands	111
IGMP Snooping Commands	115
IGMP Filtering Commands	123
Interface Commands	125
Interface Route-domain Mode	131
IP Commands	133
IP Source Binding Commands	137
IPv6 Commands	139

Layer 2 Protocol Tunnel (L2PT) Commands	163
Link Layer Discovery Protocol (LLDP) Commands	167
Load Sharing Commands	171
Logging Commands	173
Login Account Commands	175
Loopguard Commands	177
MAC Address Commands	179
MAC Authentication Commands	181
MAC Filter Commands	183
MAC Forward Commands	185
Mirror Commands	187
MRSTP Commands	191
MSTP Commands	193
Multiple Login Commands	199
MVR Commands	201
Reference N-S	203
OSPF Commands	205
Password Commands	211
PoE Commands	213
Policy Commands	217
Policy Route Commands	221
Port Security Commands	223
Port-based VLAN Commands	225
PPPoE IA Commands	227
Private VLAN Commands	233
Protocol-based VLAN Commands	237
Queuing Commands	239
RADIUS Commands	243
Remote Management Commands	245
RIP Commands	247
RMON	249
Running Configuration Commands	255
sFlow	257
Smart Isolation Commands	259
SNMP Server Commands	263
STP and RSTP Commands	267
SSH Commands	271
Static Multicast Commands	273
Static Route Commands	275
Subnet-based VLAN Commands	279
Syslog Commands	281

Reference T-Z	283
TACACS+ Commands	285
TFTP Commands	287
Trunk Commands	289
trTCM Commands	293
VLAN Commands	297
VLAN IP Commands	303
VLAN Mapping Commands	305
VLAN Port Isolation Commands	307
VLAN Stacking Commands	309
VLAN Trunking Commands	313
VRRP Commands	315
Additional Commands	319
Appendices and Index of Commands	329

PART I

Introduction

[How to Access and Use the CLI \(13\)](#)

[Privilege Level and Command Mode \(17\)](#)

[Initial Setup \(23\)](#)

How to Access and Use the CLI

This chapter introduces the command line interface (CLI).

1.1 Accessing the CLI

Use any of the following methods to access the CLI.

1.1.1 Console Port

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

Table 2 Default Settings for the Console Port

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

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

1.1.2 Telnet

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

Table 3 Default Management IP Address

SETTING	DEFAULT VALUE
IP Address	192.168.1.1
Subnet Mask	255.255.255.0

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

1.1.3 SSH

- 1 Connect your computer to one of the Ethernet ports.
- 2 Use a SSH client program to access the Switch. If this is your first login, use the default values in [Table 3 on page 13](#) and [Table 4 on page 14](#). Make sure your computer IP address is in the same subnet, unless you are accessing the Switch through one or more routers.

1.2 Logging in

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

Table 4 Default User Name and Password

SETTING	DEFAULT VALUE
User Name	admin
Password	1234



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

1.3 Using Shortcuts and Getting Help

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

Table 5 CLI Shortcuts and Help

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

1.4 Saving Your Configuration

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

```
sysname# write memory
```



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

1.5 Logging Out

Enter `logout` to log out of the CLI. You have to be in user, enable, or config mode. See [Chapter 2 on page 17](#) for more information about modes.

Privilege Level and Command Mode

This chapter introduces the CLI privilege levels and command modes.

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

2.1 Privilege Levels

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

2.1.1 Privilege Levels for Commands

The privilege level of each command is listed in the [Reference A-G](#) chapters on page 27.

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

Table 6 Types of Commands at Different Privilege Levels

PRIVILEGE LEVEL	TYPES OF COMMANDS AT THIS PRIVILEGE LEVEL
0	Display basic system information.
3	Display configuration or status.
13	Configure features except for login accounts, 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.

2.1.2 Privilege Levels for Login Accounts

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

- Using commands. Login accounts can be configured by the **admin** account or any login account with a privilege level of 14. See [Chapter 38 on page 175](#).

- Using vendor-specific attributes in an external authentication server. See the User's Guide for more information.

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

2.1.3 Privilege Levels for Sessions

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

2.1.3.1 enable Command

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

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

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

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

`password <password>`

`<password>` consists of 1-32 alphanumeric characters. For example, the following command sets the enable password to **123456**. See [Chapter 85 on page 319](#) 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 [Chapter 50 on page 211](#) for more information about this command.

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

2.1.3.2 enable <0-14> Command

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

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

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

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

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

<password> consists of 1-32 alphanumeric characters. For example, the following command sets the password for privilege level 13 to **pswd13**. See [Chapter 85 on page 319](#) for more information about this command.

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

2.1.3.3 disable Command

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

2.1.3.4 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
```

2.2 Command Modes

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

2.2.1 Command Modes for Privilege Levels 0-12

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

2.2.2 Command Modes for Privilege Levels 13-14

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

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

MODE	PROMPT	COMMAND FUNCTIONS IN THIS MODE
enable	sysname#	Display current configuration, diagnostics, maintenance.
config	sysname(config)#	Configure features other than those below.
config-interface	sysname(config-interface)#	Configure ports.
config-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 an 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 8 Changing Between Command Modes for Privilege Levels 13-14

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

2.3 Listing Available Commands

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

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

```
sysname# help
Commands available:

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

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

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

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

Initial Setup

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

3.1 Changing the Administrator Password



It is recommended you change the default administrator password. You can encrypt the password with a cipher password. See [Chapter 50 on page 211](#) for more information.

Use this command to change the administrator password.

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

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

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

3.2 Changing the Enable Password



It is recommended you change the default enable password. You can encrypt the password with a cipher password. See [Chapter 50 on page 211](#) for more information.

Use this command to change the enable password.

`password <password>`

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

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

3.3 Prohibiting Concurrent Logins

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

```
no multi-login
```

Console port has higher priority than Telnet. See [Chapter 47 on page 199](#) for more multi-login commands.

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

3.4 Changing the Management IP Address

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

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

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

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



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

3.5 Changing the Out-of-band Management IP Address

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

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

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

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

3.6 Looking at Basic System Information

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

```
show system-information
```

This is illustrated in the following example.

```
sysname# show system-information

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

See [Chapter 85 on page 319](#) for more information about these attributes.

3.7 Looking at the Operating Configuration

Use this command to look at the current operating configuration.

```
show running-config
```

This is illustrated in the following example.

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

Current configuration:

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

PART II

Reference A-G

AAA Commands (29)
ARP Commands (31)
ARP Inspection Commands (33)
ARP Learning Commands (39)
Bandwidth Commands (41)
Broadcast Storm Commands (45)
CFM Commands (49)
Classifier Commands (59)
Cluster Commands (63)
Date and Time Commands (67)
DHCP Commands (71)
DHCP Snooping & DHCP VLAN Commands (75)
DiffServ Commands (79)
Display Commands (81)
DVMRP Commands (83)
Error Disable and Recovery Commands (85)
Ethernet OAM Commands (89)
External Alarm Commands (95)
GARP Commands (97)
GVRP Commands (99)

AAA Commands

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

4.1 Command Summary

The following section lists the commands for this feature.

Table 9 aaa authentication Command Summary

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

Table 10 Command Summary: aaa accounting

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

Table 10 Command Summary: aaa accounting (continued)

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

Table 11 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 via 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 via the external server.	E	3
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 dot1x	Disables authorization of allowing an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.	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 via the external server.	C	14

ARP Commands

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

5.1 Command Summary

The following section lists the commands for this feature.

Table 12 arp Command Summary

COMMAND	DESCRIPTION	M	P
show ip arp	Displays the ARP table.	E	3
arp aging-time <60-1000000>	Enter a time from 60 to 1000000 seconds to specify how long a dynamically learned ARP entry can remain in the ARP table before it is cleared (and must be relearned).	C	13
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
no arp	Flushes the ARP table entries.	E	13

5.2 Command Examples

This example shows the ARP table.

```

sysname# show ip arp
  Index    IP             MAC                VLAN  Port    Age(s)  Type
  ----    -             -                -    -    -    -
    1      192.168.1.1    00:19:cb:6f:91:59    1    CPU      0      static
sysname#

```

The following table describes the labels in this screen.

Table 13 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.

Table 13 show ip arp (continued)

LABEL	DESCRIPTION
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.

ARP Inspection Commands

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

6.1 Command Summary

The following section lists the commands for this feature.

Table 14 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 VLAN(s).	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 VLAN(s).	E	3

Table 15 Command Summary: arp inspection filter

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

Table 16 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 17 Command Summary: interface arp inspection

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

Table 18 Command Summary: arp inspection vlan

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

6.2 Command Examples

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

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

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

The following table describes the labels in this screen.

Table 19 show arp inspection filter

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

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

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

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

The following table describes the labels in this screen.

Table 20 show arp inspection log

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

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

```

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

```

The following table describes the labels in this screen.

Table 21 show arp inspection interface port-channel

LABEL	DESCRIPTION
Interface	This field displays the port number. If you configure the * port, the settings are applied to all of the ports.
Trusted State	This field displays whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are connected to DHCP servers or other switches, and the switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high.
Rate (pps)	This field displays the maximum number for DHCP packets that the switch receives from each port each second. The switch discards any additional DHCP packets.
Burst Interval	This field displays the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the switch accepts a maximum of 75 ARP packets in every five-second interval.

ARP Learning Commands

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

7.1 Command Summary

The following section lists the commands for this feature.

Table 22 arp-learning Command Summary

COMMAND	DESCRIPTION	M	P
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s).	C	13
<code>arp-learning <arp-reply gratuitous-arp arp-request></code>	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
<code>no arp-learning</code>	Resets the ARP learning mode to its default setting (arp-reply).	C	13

7.2 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
```


Bandwidth Commands

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



Bandwidth management implementation differs across Switch models.

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

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



The CIR should be less than the PIR.

See [Section 8.2 on page 42](#) and [Section 8.3 on page 43](#) for examples.

See also [Chapter 77 on page 293](#) for information on how to use trTCM (Two Rate Three Color Marker) to control traffic flow.

8.1 Command Summary

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

Table 23 User-input Values: running-config

COMMAND	DESCRIPTION
<i>port-list</i>	The port number or a range of port numbers that you want to configure.
<i>rate</i>	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 24 Command Summary: bandwidth-control & bandwidth-limit

COMMAND	DESCRIPTION	M	P
<code>show interfaces config <port-list> bandwidth-control</code>	Displays the current settings for interface bandwidth control.	E	3
<code>bandwidth-control</code>	Enables bandwidth control on the Switch.	C	13
<code>no bandwidth-control</code>	Disables bandwidth control on the Switch.	C	13
<code>interface port-channel <port-list></code>	Enters subcommand mode for configuring the specified ports.	C	13
<code>bandwidth-limit ingress</code>	Enables bandwidth limits for incoming traffic on the port(s).	C	13
<code>bandwidth-limit ingress <rate></code>	Sets the maximum bandwidth allowed for incoming traffic on the port(s).	C	13
<code>bandwidth-limit egress</code>	Enables bandwidth limits for outgoing traffic on the port(s).	C	13
<code>bandwidth-limit egress <rate></code>	Sets the maximum bandwidth allowed for outgoing traffic on the port(s).	C	13
<code>no bandwidth-limit ingress</code>	Disables ingress bandwidth limits on the specified port(s).	C	13
<code>no bandwidth-limit egress</code>	Disables egress bandwidth limits on the specified port(s).	C	13
<code>bandwidth-limit cir</code>	Enables commit rate limits on the specified port(s).	C	13
<code>bandwidth-limit cir <rate></code>	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
<code>bandwidth-limit pir</code>	Enables peak rate limits on the specified port(s).	C	13
<code>bandwidth-limit pir <rate></code>	Sets the maximum bandwidth allowed for the incoming traffic flow on the specified port(s).	C	13
<code>no bandwidth-limit cir</code>	Disables commit rate limits on the specified port(s).	C	13
<code>no bandwidth-limit pir</code>	Disables peak rate limits on the specified port(s).	C	13

8.2 Command Examples: ingress

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

```

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

```

This example deactivates the outgoing bandwidth limit on port 1.

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

8.3 Command Examples: cir & pir

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

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

This example displays the bandwidth limits configured on port 1.

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

Current configuration:

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


Broadcast Storm Commands

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



Broadcast storm control implementation differs across Switch models.

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

See [Section 9.2 on page 46](#) and [Section 9.3 on page 46](#) for examples.

9.1 Command Summary

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

Table 25 User-input Values: broadcast-limit, multicast-limit & dlf-limit

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

The following section lists the commands for this feature.

Table 26 Command Summary: storm-control, bmstorm-limit, and bstorm-control

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

Table 26 Command Summary: storm-control, bmstorm-limit, and bstorm-control (continued)

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

9.2 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

```

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

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

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

- **64** DLF packets per second.

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

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

CFM Commands

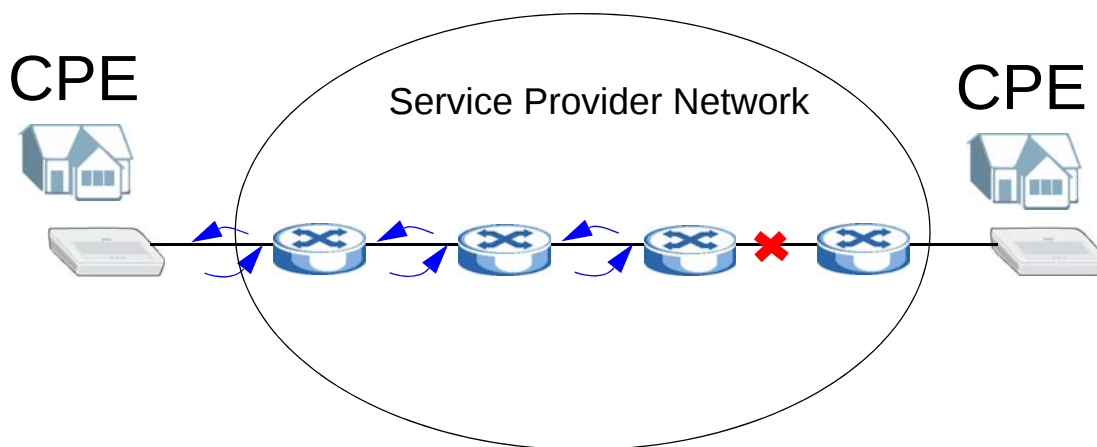
Use these commands to configure the Connectivity Fault Management (CFM) on the Switch.

10.1 CFM Overview

The route between two users may go through aggregated switches, routers and/or DSLAMs owned by independent organizations. A connectivity fault point generally takes time to discover and impacts subscribers' network access. IEEE 802.1ag is a Connectivity Fault Management (CFM) specification which allows network administrators to identify and manage connection faults in order to ease management and maintenance. Through discovery and verification of the path, CFM can detect and analyze connectivity faults in bridged LANs.

The figure shown below is an example of a connection fault between switches in the service provider's network. CFM can be used to identify and management this kind of connection problem.

Figure 1 Connectivity Fault Example



10.1.1 How CFM Works

CFM sends pro-active Connectivity Check (CC) packets between two CFM-aware devices in the same MD (Maintenance Domain) network. An MA (Maintenance Association) defines a VLAN and associated ports on the device under an MD level. In this MA, a port can be an MEP (Maintenance End Point) port or an MIP (Maintenance Intermediate Point) port.

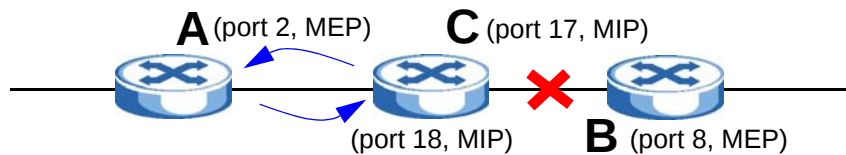
- MEP port - has the ability to send pro-active connectivity check (CC) packets and get other MEP port information from neighbor switches' CC packets within an MA.
- MIP port - only forwards the CC packets.

CFM provides two tests to discover connectivity faults.

- Loopback test - similar to using “ping” in Microsoft DOS mode to check connectivity from your computer to a host. In a loopback test, a MEP port sends a LBM (Loop Back Message) to a MIP port and checks for an LBR (Loop Back Response). If no response is received, there might be a connectivity fault between them.
- Link trace test - similar to using “tracert” in the Microsoft DOS mode to check connectivity from your computer to a host. A link trace test provides additional connectivity fault analysis to get more information on where the fault is. In a link trace test, a MEP port sends a LTM (Link Trace Message) to a MIP port and checks for an LTR (Link Trace Response). If an MIP or MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check the fault and resume services according to the line connectivity status report.

An example is shown next. A user cannot access the Internet. To check the problem, the administrator starts the link trace test from **A** which is an MEP port to **B** which is also an MEP port. Each aggregation MIP port between aggregated devices responds to the LTM packets and also forwards them to the next port. A fault occurs at port **C**. **A** discovers the fault since it only gets the LTR packets from the ports before port **C**.

Figure 2 MIP and MEP Example



10.2 CFM Term Definition

This section lists the common term definition which appears in this chapter. Refer to User's Guide for more detailed information about CFM.

Table 27 CFM Term Definitions

TERM	DESCRIPTION
CFM	CFM (Connectivity Fault Management) is used to detect and analyze connectivity faults in bridged LANs.
MD	An MD (Maintenance Domain) is part of a network, where CFM can be done. The MD is identified by a level number and contains both MEPs and MIPs. The Switch supports up to eight MD levels (0 ~ 7) in a network. You can create multiple MDs on one MD level and multiple MA groups in one MD.
MA	An MA (Maintenance Association) is a group of MEPs and identified by a VLAN ID. One MA should belong to one and only one MD group.

Table 27 CFM Term Definitions

TERM	DESCRIPTION
MEP	An MEP (Maintenance End Point) port has the ability to send and reply to the CCMs, LBMs and LTMs. It also gets other MEP port information from neighbor switches' CCMs in an MA.
MIP	An MIP (Maintenance Intermediate Point) port forwards the CCMs, LBMs, and LTMs and replies the LBMs and LTMs by sending Loop Back Responses (LBRs) and Link Trace Responses (LTRs).
Connectivity Check	Connectivity Check (CC) enables an MEP port sending Connectivity Check Messages (CCMs) periodically to other MEP ports. An MEP port collects CCMs to get other MEP information within an MA.
Loop Back Test	Loop Back Test (LBT) checks if an MEP port receives its LBR (Loop Back Response) from its target after it sends the LBM (Loop Back Message). If no response is received, there might be a connectivity fault between them.
Link Trace Test	Link Trace Test (LTT) provides additional connectivity fault analysis to get more information on where the fault is. In the link trace test, MIP ports also send LTR (Link Trace Response) to response the source MEP port's LTM (Link Trace Message). If an MIP or MEP port does not respond to the source MEP, this may indicate a fault. Administrators can take further action to check and resume services from the fault according to the line connectivity status report.

10.3 User Input Values

This section lists the common term definition appears in this chapter. Refer to User's Guide for more detailed information about CFM.

Table 28 CFM command user input values

USER INPUT	DESCRIPTION
<i>mep-id</i>	This is the maintenance endpoint identifier (1~8191).
<i>ma-index</i>	This is the maintenance association (MA) index number (1~4294967295).
<i>md-index</i>	This is the maintenance domain (MD) index number (1~4294967295).
<i>mac-address</i>	This is the remote maintenance endpoint's MAC address or a virtual MAC address assigned to a port. A switch has one or two MAC addresses only. If you do not use virtual MAC addresses with CFM, all CFM ports will use the Switch's MAC address and appear as one port. If you want unique CFM ports, you need to assign virtual MAC addresses. If you use virtual MAC addresses, make sure that all virtual MAC addresses are unique in both the switch and the network to which it belongs.

10.4 Command Summary

The following section lists the commands for this feature.

Table 29 CFM Command Summary

COMMAND	DESCRIPTION	M	P
<code>clear ethernet cfm linktrace</code>	Clears the link trace database.	E	13
<code>clear ethernet cfm mep-ccmdb</code>	Clears the MEP CCM database.	E	13
<code>clear ethernet cfm mip-ccmdb</code>	Clears the MIP CCM database.	E	13
<code>clear ethernet cfm mep-defects</code>	Clears the MEP-defects database.	E	13
<code>ethernet cfm</code>	Enables CFM on the Switch.	C	13
<code>ethernet cfm loopback remote-mep <mep-id> mep <mep-id> ma <ma-index> md <md-index> [size <0-1500>][count <1-1024>]</code>	Specifies the remote MEP ID, local MEP ID, MA index and MD index to perform a loopback test. This enables the MEP port (with the specified MEP ID) in a specified CFM domain to send the LBMs (Loop Back Messages) to a specified remote end point. You can also define the packet size (from 0 to 1500 bytes) and how many times the Switch sends the LBMs.	E	13
<code>ethernet cfm loopback mac <mac-address> mep <mep-id> ma <ma-index> md <md-index> [size <0-1500>][count <1-1024>]</code>	Specifies the destination MAC address, local MEP ID, MA index and MD index to perform a loopback test. This enables the MEP port (with the specified MEP ID) in a specified CFM domain to send the LBMs (Loop Back Messages) to a specified remote end point. You can also define the packet size (from 0 to 1500 bytes) and how many times the Switch sends the LBMs.	E	13
<code>ethernet cfm linktrace remote-mep <mep-id> mep <mep-id> ma <ma-index> md <md-index> [mip-ccmdb][ttl <ttl>]</code>	Specifies the remote MEP ID, local MEP ID, MA index and MD index to perform a link trace test. This enables the MEP port (with the specified MEP ID) in a specified CFM domain to send the LTMs (Link Trace Messages) to a specified remote end point. <i>mip-ccmdb</i> : Specifies the MIP CCM DB, a database that stores information (tuples of {Port, VID, MAC address}) about MEPs in the MD when receiving CCMs. The MIP CCM DB is used for fault isolation, such as link trace and loop back. An entry can remain in the MIP CCM DB for at least 24 hours. <i>ttl</i> : This is the time-to-live value (the number of transmissions, 64 hops by default). Sets this to stop a test once it exceeds the time duration without receiving any response.	E	13
<code>ethernet cfm linktrace mac <mac-address> mep <mep-id> ma <ma-index> md <md-index> [mip-ccmdb][ttl <ttl>]</code>	Specifies the destination MAC address, local MEP ID, MA index and MD index to perform a link trace test. This enables the MEP port (with the specified MEP ID) in a specified CFM domain to send the LTMs (Link Trace Messages) to a specified remote end point. <i>mip-ccmdb</i> : Specifies the MIP CCM DB, a database that stores information (tuples of {Port, VID, MAC address}) about MEPs in the MD when receiving CCMs. The MIP CCM DB is used for fault isolation, such as link trace and loop back. An entry can remain in the MIP CCM DB for at least 24 hours. <i>ttl</i> : This is the time-to-live value (the number of transmissions, 64 hops by default). Sets this to stop a test once it exceeds the time duration without receiving any response.	E	13

Table 29 CFM Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ethernet cfm ma <ma-index> format <vid string integer> name <ma-name> md <md-index> primary-vlan <1-4094>	Creates an MA (Maintenance Association) and defines its VLAN ID under the MD. You can also define the format which the Switch uses to send this MA information in the domain (MD). <i>ma-name</i> : Enters a VLAN ID, a descriptive name or a 2-octet integer for the MA. Note: If you set the format to vid, the VLAN ID should be the same as the VLAN ID you use to identify the MA.	C	13
cc-interval <100ms 1s 10s 1min 10min>	Sets how often an MEP sends a connectivity check message (CCM).	C	13
mhf-creation < none default explicit>	Sets MHF (MIP Half Function). Select none and no MIP can be created automatically for this MA. Select default to automatically create MIPs for this MA and on the ports belonging to this MA's VLAN when there are no lower configured MD levels or there is an MEP at the next lower configured MD level on the port. Select explicit to automatically create MIPs for this MA and on the ports belonging to this MA's VLAN only when there is an MEP at the next lower configured MD level on the port.	C	13
id-permission < none chassis management chassis-management>	Sets what's to be included in the sender ID TLV (Type-Length-Value) transmitted by CFM packets. Select none to not include the sender ID TLV. Select chassis to include the chassis information. Select management to include the management information. Select chassis-management to include both chassis and management information.	C	13
exit	Exits from the config-ma mode.	C	13
remote-mep <mep-id>	Sets a remote MEP in an MA.	C	13
mep <mep-id> interface port-channel <port> direction <up down> priority <0-7>	Sets an MEP in an MA. up down: The traffic direction. 0-7: The priority value of the CCMs or LTMs transmitted by the MEP. 1 is the lowest, then 2, 0 and 3 ~ 7.	C	13
mep <mep-id> interface port-channel <port> direction <up down> priority <0-7> inactive	Disables a specified MEP.	C	13
mep <mep-id> interface port-channel <port> direction <up down> priority <0-7> cc-enable	Enables Connectivity Check (CC) to allow an MEP sending Connectivity Check Messages (CCMs) periodically to other MEPs.	C	13
no remote-mep <mep-id>	Deletes a specified destination MEP.	C	13
no mep <mep-id>	Deletes a specified MEP.	C	13
no mep <mep-id> inactive	Enables an MEP.	C	13
no mep <mep-id> cc-enable	Disallows an MEP sending Connectivity Check Messages (CCMs) periodically to other MEPs.	C	13

Table 29 CFM Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ethernet cfm md <md-index> format <dns mac string> name <md-name> level <0-7>	Creates an MD (Maintenance Domain) with the specified name and level number. <i>md-name</i> : Enters a domain name, MAC address or a descriptive name for the MD.	C	13
ethernet cfm management-address-domain ip [<ip-addr>]	Sets the Switch to carry the host name and management IP address for the VLAN to which an MEP belongs or the specified IP address in CFM packets. This helps you to easily identify a remote MEP by its host name and management IP address showed in the link trace database and MEP-CCM database.	C	13
interface port-channel <port-list>	Enters config-interface mode for configuring the specified port(s).	C	13
ethernet cfm virtual-mac <mac-addr>	Assigns a virtual MAC address(es) to the specified port(s) so that each specified port can have its own MAC address for CFM. You cannot use the copy running-config interface port-channel command to copy the virtual MAC address from the specified port to other ports.	C	13
no ethernet cfm virtual-mac	Removes the virtual MAC address(es) and sets the port(s) to use the default system MAC address.	C	13
no ethernet cfm	Disables CFM on the Switch.	C	13
no ethernet cfm md <md-index>	Deletes the specified MD.	C	13
no ethernet cfm ma <ma-index> md <md-index>	Deletes an MA from the specified MD.	C	13
no ethernet cfm management-address-domain	Sets the Switch to not carry the host name and management IP address in CFM packets.	C	13
show ethernet cfm linktrace	Displays the CFM link trace database information.	E	13
show ethernet cfm local	Displays the detailed settings of the configured MD(s) and MA(s).	E	13
show ethernet cfm local stack	Displays a list of all maintenance points, such as MIP and MEP.	E	13
show ethernet cfm local stack mep	Displays a list of the MEP(s).	E	13
show ethernet cfm local stack mep <mep-id> ma <ma-index> md <md-index>	Displays the specified MEP's general, fault notification generator, continuity-check, loopback and link trace information.	E	13
show ethernet cfm local stack mep <mep-id> ma <ma-index> md <md-index> mep-ccmdb [remote-mep <mep-id>]	Displays the specified MEP's MEP-CCM database information. Each MEP maintains an MEP CCM database which stores information about remote MEPs in the MA when receiving CCMs.	E	13
show ethernet cfm local stack mip	Displays a list of the MIP(s).	E	13
show ethernet cfm local stack mip mip-ccmdb	Displays the MIP-CCM database.	E	13
show ethernet cfm remote	Displays a list of MA(s), MEP(s) and the remote MEP(s) under the configured MD(s).	E	13
show ethernet cfm virtual-mac	Displays all virtual MAC addresses.	E	13
show ethernet cfm virtual-mac port <port-list>	Displays the MAC address(es) of the specified port(s).	E	13

10.5 Command Examples

This example creates **MD1** (with MD index 1 and level 1) and **MA2** (with MA index 2 and VLAN ID 2) under **MD1** that defines a CFM domain.

```
sysname# config
sysname(config)# ethernet cfm md 1 format string name MD1 level 1
sysname(config)# ethernet cfm ma 2 format string name MA2 md 1 primary-
vlan 2
sysname(config-ma)# exit
sysname(config)# exit
sysname# write memory
```



Remember to save new settings using the `write memory` command.

This example deletes **MA2** (with MA index 2) from **MD1** (with MD index 1).

```
sysname# config
sysname(config)# no ethernet cfm ma 2 md 1
sysname(config)# exit
sysname# write mem
```

This example creates **MA3** (with MA index 3 and VLAN ID 123) under **MD1**, and associates port 1 as an MEP port with MEP ID 301 in the specified CFM domain. This also sets MHF (MIP half function) to **default** to have the Switch automatically create MIPs for this MA and on the ports belonging to this MA's VLAN when there are no lower configured MD levels or there is a MEP at the next lower configured MD level on the port. This also sets a remote MEP in **MA3**.

```
sysname# config
sysname(config)# ethernet cfm ma 3 format string name MA3 md 1 primary-vlan
123
sysname(config-ma)# mep 301 interface port-channel 1 direction up priority 2
sysname(config-ma)# mep 301 interface port-channel 1 direction up priority 2
cc-enable
sysname(config-ma)# mhf-creation default
sysname(config-ma)# remote-mep 117
sysname(config-ma)# exit
sysname(config)# exit
sysname# write mem
```

This example lists all CFM domains. In this example, only one MD (**MD1**) is configured. The **MA3** with the associated MEP port 1 is under this **MD1**.

```
sysname# show ethernet cfm local
MD Index: 1
  MD Name: MD1(string)
  MD Level: 1
    MA Index: 3
      MA Name:          MA3(string)
      Primary Vlan:     123
      CC Interval:      1000 millisecond(s)
      MHF Creation:     default
      ID Permission:    none
      MEP:301 (ACTIVE ) Port:1   Direction:DOWN Priority:5 CC-Enable:FALSE
sysname#
```

This example starts a loopback test and displays the test result on the console.

```
sysname# ethernet cfm loopback remote-mep 2 mep 1 ma 1 md 1
Sending 5 Ethernet CFM Loopback messages to remote-mepid 2, timeout is 5
seconds .....
sysname# Loopback: Successful
Success rate is 100 percent, round-trip min/avg/max = 0/0/0 ms
sysname#
```

This example displays all neighbors' MEP port information in the MIP-CCM databases.

```
sysname# show ethernet cfm local stack mip mip-ccmdb
MIP CCM DB
Port  VID      Source Address      Retained
----  -
  2    1    00:19:cb:00:00:04    0 hr(s)
  7    1    00:19:cb:00:00:06    0 hr(s)
sysname#
```

The following table describes the labels in this screen.

Table 30 show cfm-action mipccmdb

LABEL	DESCRIPTION
Port	Displays the number of the port on which this CCM was received.
VID	Displays the MA VLAN ID of the last received CCM.
Source Address	Displays the MAC address of the remote MEP.
Retained	Displays how long an entry has been kept in the database.

This example assigns a virtual MAC address to port 3 and displays the MAC addresses of the ports 2 ~ 4. The assigned virtual MAC address should be unique in both the Switch and the network to which it belongs.

```
sysname# config
sysname(config)# interface port-channel 3
sysname(config-interface)# ethernet cfm virtual-mac 00:19:cb:12:34:56
sysname(config-interface)# exit
sysname(config)# exit
sysname# show ethernet cfm virtual-mac port 2-4
Virtual MACPort MAC
-----
2      00:19:cb:00:00:02
3      00:19:cb:12:34:56
4      00:19:cb:00:00:02
sysname#
```

This example sets the Switch to carry its host name and management IP address 192.168.100.1 in CFM packets.

```
sysname# config
sysname(config)# ethernet cfm management-address-domain ip 192.168.100.1
```

This example shows remote MEP database information. The remote MEP has been configured to carry its host name and a specified IP address in CFM packets.

```
sysnam# show ethernet cfm remote
MD Index: 1
MD Name: customer123(string)
MD Level: 2
MA Index: 1
MA Name: 123(vid)
Primary Vlan: 123
MEP: 11
Remote MEP ID: 1
MAC Address: 00:19:cb:6f:91:5a
Chassis Id: MGS-3712F
Management Address: 192.168.100.1:161
sysname#
```


Classifier Commands

Use these commands to classify packets into traffic flows. After classifying traffic, policy commands ([Chapter 52 on page 217](#)) can be used to ensure that a traffic flow gets the requested treatment in the network.

11.1 Command Summary

The following section lists the commands for this feature.

Table 31 Command Summary: classifier

COMMAND	DESCRIPTION	M	P
show classifier [<i><name></i>]	Displays classifier configuration details.	E	3
classifier <i><name></i> [<packet-format <802.3untag 802.3tag EtherIIuntag EtherIItag>] [priority <0-7>] [vlan <vlan-id>] [ethernet-type <ether-num ip ipx arp rarp appletalk ecnet ipv6>] [source-mac <src-mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [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] [source-ip <src-ip-addr>] [mask-bits <mask-bits>] [ipv6-source-ip <src-ipv6-addr>] [prefix-length <prefix-length>] [source-socket <socket-num>] [destination-ip <dest-ip-addr>] [mask-bits <mask-bits>] [ipv6-destination-ip <dest-ipv6-addr>] [prefix-length <prefix-length>] [destination-socket <socket-num>] [inactive]>	Configures a classifier. Specify the parameters to identify the traffic flow: ethernet-type - enter one of the Ethernet types or type the hexadecimal number that identifies an Ethernet type (see Table 32 on page 60) ip-protocol : enter one of the protocols or type the port number that identifies the protocol (see Table 33 on page 60) establish-only : enter this to identify only TCP packets used to establish TCP connections. source-socket : (for UDP or TCP protocols only) specify the protocol port number. destination-socket : (for UDP or TCP protocols only) specify the protocol port number. inactive : disables this classifier. ipv6-next-header : enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255 (see Table 34 on page 60). See Chapter 33 on page 139 for more information about IPv6.	C	13
no classifier <i><name></i>	Deletes the classifier. If you delete a classifier you cannot use policy rule related information.	C	13
no classifier <i><name></i> inactive	Enables a classifier.	C	13

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

Table 32 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 33 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 34 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

Table 34 Common IPv6 Next Header Values

PROTOCOL TYPE	VALUE
No Next Header for IPv6	59
Destination Options for IPv6	60

11.2 Command Examples

This example creates a classifier for packets with a VLAN ID of 3. The resulting traffic flow is identified by the name **VLAN3**. The **policy** command can use the name **VLAN3** to apply policy rules to this traffic flow. See the policy example in [Chapter 52 on page 217](#).

```
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 52 on page 217](#).

```
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...
```


Cluster Commands

Use these commands to configure cluster management.

12.1 Command Summary

The following section lists the commands for this feature.

Table 35 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 member(s) and their running status.	E	3
show cluster member config	Displays the current cluster member(s).	E	3
show cluster member mac <mac>	Displays the running status of the cluster member(s).	E	3
cluster rcommand <mac>	Logs into the CLI of the specified cluster member.	C	13
no cluster member <mac>	Removes the cluster member.	C	13

12.2 Command Examples

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

```

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

```

The following table describes the labels in this screen.

Table 36 show cluster member

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

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

```

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

User name: admin

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

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

Closed
sysname(config)#

```

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

```

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

```

The following table describes the labels in this screen.

Table 37 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.

Date and Time Commands

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

13.1 Command Summary

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

Table 38 time User-input Values

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

The following section lists the commands for this feature.

Table 39 time Command Summary

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

Table 39 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 <i>o'clock</i> 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 <i>o'clock</i> 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 40 timesync Command Summary

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

13.2 Command Examples

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

```

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

```

This example looks at the current time server settings.

```
sysname# show timesync

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

Time Server Sync Status:CONNECTING
```

The following table describes the labels in this screen.

Table 41 show timesync

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

DHCP Commands

Use these commands to configure DHCP features on the Switch.

- Use the `dhcp relay` commands to configure DHCP relay for specific VLAN.
- Use the `dhcp smart-relay` commands to configure DHCP relay for all broadcast domains.
- Use the `dhcp server` commands to configure the Switch as a DHCP server. (This command is available on a layer 3 switch only.)

14.1 Command Summary

The following section lists the commands for this feature.

Table 42 dhcp smart-relay Command Summary

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

Table 43 dhcp relay Command Summary

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

Table 44 dhcp relay-broadcast Command Summary

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

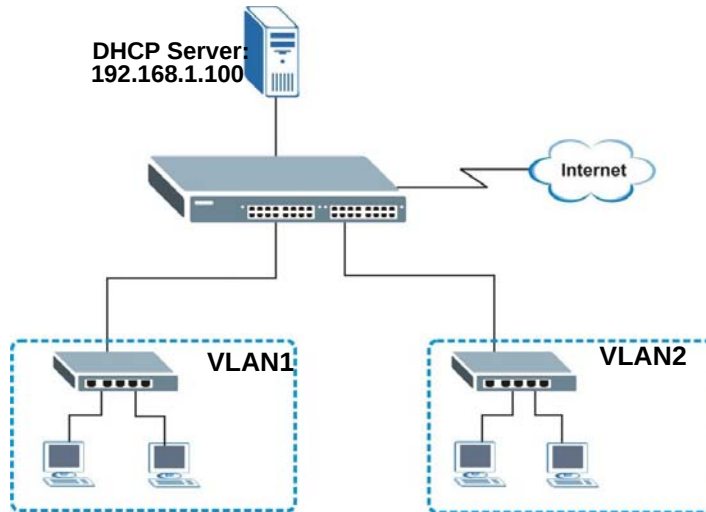
Table 45 dhcp server Command Summary

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

14.2 Command Examples

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

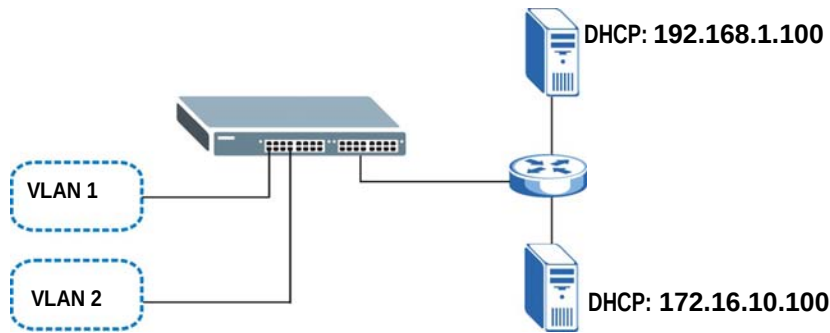
Figure 3 Example: Global DHCP Relay



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
```

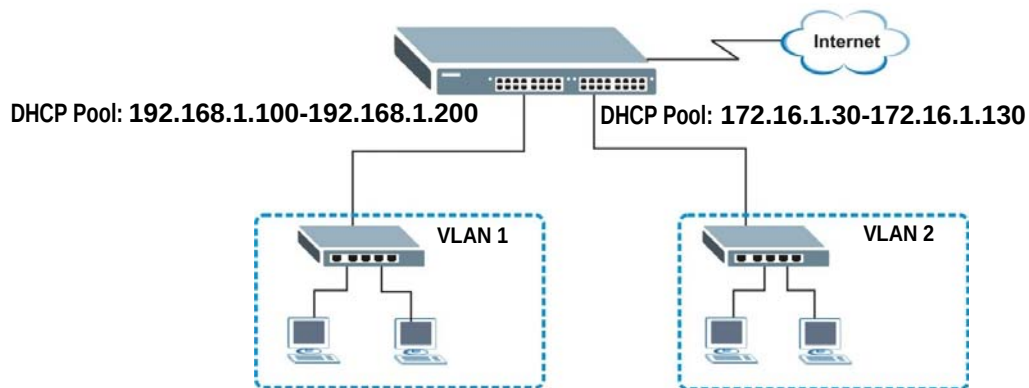
In this example, there are two VLANs (VIDs 1 and 2) in a campus network. Two DHCP servers are installed to serve each VLAN. The Switch forwards DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with IP address 192.168.1.100. DHCP requests from the academic buildings (VLAN 2) are sent 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 74](#). 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
```

DHCP Snooping & DHCP VLAN Commands

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

15.1 Command Summary

The following section lists the commands for this feature.

Table 46 dhcp snooping Command Summary

COMMAND	DESCRIPTION	M	P
<code>show dhcp snooping</code>	Displays DHCP snooping configuration on the Switch.	E	3
<code>show dhcp snooping binding</code>	Displays the DHCP binding table.	E	3
<code>show dhcp snooping database</code>	Displays DHCP snooping database update statistics and settings.	E	3
<code>show dhcp snooping database detail</code>	Displays DHCP snooping database update statistics in full detail form.	E	3
<code>dhcp snooping</code>	Enables DHCP Snooping on the Switch.	C	13
<code>no dhcp snooping</code>	Disables DHCP Snooping on the Switch.	C	13
<code>dhcp snooping database <tftp://host/filename></code>	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
<code>no dhcp snooping database</code>	Removes the location of the DHCP snooping database.	C	13
<code>dhcp snooping database timeout <seconds></code>	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
<code>no dhcp snooping database timeout <seconds></code>	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
<code>dhcp snooping database write-delay <seconds></code>	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
<code>no dhcp snooping database write-delay <seconds></code>	Resets how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update to the default value (300).	C	13

Table 46 dhcp snooping Command Summary (continued)

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

The following table describes the dhcp-vlan commands.

Table 47 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

15.2 Command Examples

This example:

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

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

```

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

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

```


DiffServ Commands

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

16.1 Command Summary

The following section lists the commands for this feature.

Table 48 diffserv Command Summary

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

Display Commands

Use these commands to display configuration information.

17.1 Command Summary

The following section lists the commands for this feature.

Table 49 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

DVMRP Commands

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

18.1 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.

18.2 Command Summary

The following section lists the commands for this feature.

Table 50 Command Summary: DVMRP

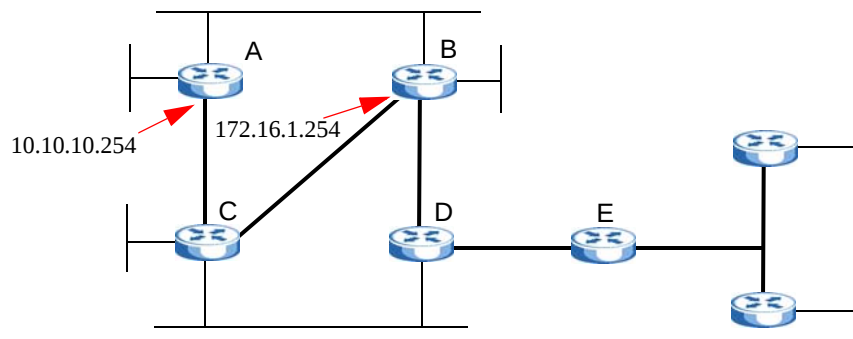
COMMAND	DESCRIPTION	M	P
show ip dvmrp group	Displays DVMRP group information.	E	3
show ip dvmrp interface	Displays DVMRP interface information.	E	3
show ip dvmrp neighbor	Displays DVMRP neighbor information.	E	3
show ip dvmrp prune	Displays the DVMRP prune information.	E	3
show ip dvmrp route	Displays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

Table 50 Command Summary: DVMRP (continued)

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

18.3 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

Error Disable and Recovery Commands

Use these commands to configure the CPU protection and error disable recovery features on the Switch.

19.1 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 network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

19.2 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 port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

19.3 User Input Values

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

Table 51 errdisable recovery command user input values

USER INPUT	DESCRIPTION
<i>port-list</i>	The port number or a range of port numbers that you want to configure.

19.4 Command Summary

The following section lists the commands for this feature.

Table 52 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 port(s) 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 port(s) 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 port(s) to handle all ARP, BPDU or IGMP packets in stead of ignoring them, if the port(s) are in inactive-reason mode (set by using the errdisable detet 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 port(s).	E	13

Table 53 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 port(s) (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 port(s). 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 port(s) 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>	Enables the recovery timer for the specified feature that causes the Switch to shut down port(s).	C	13
errdisable recovery cause <loopguard ARP BPDU IGMP> interval <30-2592000>	Sets how many seconds the Switch waits before enabling the port(s) which was shut down.	C	13
no errdisable detect cause <ARP BPDU IGMP>	Disables the rate limit for ARP, BPDU or IGMP packets on port(s), 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>	Disables the recovery timer for the specified feature that causes the Switch to shut down a port.	C	13

Table 53 errdisable recovery Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show errdisable	Displays which port(s) 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 port(s) will be activated.	E	13

19.5 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.

```

systemname# config
systemname(config)# interface port-channel 7
systemname(config-interface)# cpu-protection cause ARP rate-limit 100
systemname(config-interface)# exit
systemname(config)# errdisable detect cause ARP
systemname(config)# errdisable detect cause ARP mode inactive-port
systemname(config)# exit
systemname# 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      -

systemname# show errdisable detect

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

```

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 port(s) and the time left before the port(s) 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

Interfaces that will be enabled at the next timeout:

Interface	Reason	Time left(sec)	Mode
-----	-----	-----	-----

```
sysname#
```

Ethernet OAM Commands

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

20.1 IEEE 802.3ah Link Layer Ethernet OAM Implementation

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

The Switch supports the following IEEE 802.3ah features:

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

20.2 Command Summary

The following section lists the commands for this feature.

Table 54 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
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

Table 54 ethernet oam Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 port(s).	C	13
ethernet oam	Enables Ethernet OAM on the port(s).	C	13
no ethernet oam	Disables Ethernet OAM on the port(s).	C	13
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

20.3 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 55 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.

Table 55 show ethernet oam discovery (continued)

LABEL	DESCRIPTION
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.
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 connection. 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 56 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.
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 57 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.

Table 57 show ethernet oam summary (continued)

LABEL	DESCRIPTION
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.

External Alarm Commands

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

21.1 Command Summary

The following section lists the commands for this feature.

Table 58 external-alarm Command Summary

COMMAND	DESCRIPTION	M	P
external-alarm <index> name <name_string>	Sets the name of the specified external alarm. <i>index</i> : 1 ~ 4 <i>name_string</i> : 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

21.2 Command Examples

This example configures and shows the name and status of the external alarm(s).

```
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#
```

GARP Commands

Use these commands to configure GARP.

22.1 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.

22.2 Command Summary

The following section lists the commands for this feature.

Table 59 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

22.3 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
```

GVRP Commands

Use these commands to configure GVRP.

23.1 Command Summary

The following section lists the commands for this feature.

Table 60 gvrp Command Summary

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

23.2 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

[HTTPS Server Commands \(103\)](#)
[IEEE 802.1x Authentication Commands \(107\)](#)
[IGMP and Multicasting Commands \(111\)](#)
[IGMP Snooping Commands \(115\)](#)
[IGMP Filtering Commands \(123\)](#)
[Interface Commands \(125\)](#)
[Interface Route-domain Mode \(131\)](#)
[IP Commands \(133\)](#)
[IP Source Binding Commands \(137\)](#)
[IPv6 Commands \(139\)](#)
[Layer 2 Protocol Tunnel \(L2PT\) Commands \(163\)](#)
[Link Layer Discovery Protocol \(LLDP\) Commands \(167\)](#)
[Load Sharing Commands \(171\)](#)
[Logging Commands \(173\)](#)
[Login Account Commands \(175\)](#)
[Loopguard Commands \(177\)](#)
[MAC Address Commands \(179\)](#)
[MAC Authentication Commands \(181\)](#)
[MAC Filter Commands \(183\)](#)
[MAC Forward Commands \(185\)](#)
[Mirror Commands \(187\)](#)
[MRSTP Commands \(191\)](#)
[MSTP Commands \(193\)](#)

Multiple Login Commands (199)

MVR Commands (201)

HTTPS Server Commands

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

24.1 Command Summary

The following section lists the commands for this feature.

Table 61 https Command Summary

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

24.2 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 62 show https

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

Table 62 show https (continued)

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

This example shows the current HTTPS sessions.

```

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

```

The following table describes the labels in this screen.

Table 63 show https session

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

Table 63 show https session (continued)

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

IEEE 802.1x Authentication Commands

Use these commands to configure IEEE 802.1x authentication.



Do not forget to configure the authentication server.

25.1 Guest VLAN Overview

When 802.1x port authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the port(s). You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN on a port, the user that is not IEEE 802.1x capable or fails to enter the correct username and password can still access the port, but traffic from the user is forwarded to the guest VLAN. That is, unauthenticated users can have access to limited network resources in the same guest VLAN, such as the Internet. The rights granted to the guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

25.2 Command Summary

The following section lists the commands for this feature.

Table 64 port-access-authenticator Command Summary

COMMAND	DESCRIPTION	M	P
no port-access-authenticator	Disables port authentication on the Switch.	C	13
no port-access-authenticator <port-list>	Disables authentication on the listed ports.	C	13
no port-access-authenticator <port-list> reauthenticate	Disables the re-authentication mechanism on the listed port(s).	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 802.1x authentication on the Switch.	C	13

Table 64 port-access-authenticator Command Summary (continued)

COMMAND	DESCRIPTION	M	P
port-access-authenticator <port-list>	Enables 802.1x authentication on the specified port(s).	C	13
port-access-authenticator <port-list> guest-vlan	Enables the guest VLAN feature on the listed ports.	C	13
port-access-authenticator <port-list> guest-vlan <vlan-id>	Sets the guest VLAN ID number on the listed ports.	C	13
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 port 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 [<1-24>]	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 port(s).	C	13
port-access-authenticator <port-list> max-req <1-10>	Sets the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the guest VLAN.	C	13
port-access-authenticator <port-list> quiet-period <0-65535>	Sets the number of seconds the port(s) 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 challenge 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 identity request to clients on the listed ports.	C	13
port-access-authenticator <port-list> reauthenticate	Sets a subscriber to periodically re-enter his or her username and password to stay connected to a specified port.	C	13
port-access-authenticator <port-list> reauth-period <1-65535>	Specifies how often (in seconds) a client has to re-enter the username and password to stay connected to the specified port(s).	C	13
show port-access-authenticator	Displays all port authentication settings.	E	3
show port-access-authenticator <port-list>	Displays port authentication settings on the specified port(s).	E	3

25.3 Command Examples

This example configures the Switch in the following ways:

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

- 5 Activates reauthentication on ports 4-8.
- 6 Specifies 1800 seconds as the interval for client reauthentication on ports 4-8.

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

This example configures the Switch in the following ways:

- 1 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
```


IGMP and Multicasting Commands

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

26.1 IGMP Overview

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

26.2 Command Summary

The following section lists the commands for this feature.

Table 65 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 65 IGMP Command Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>ip igmp robustness-variable <2-255></code>	Sets the IGMP robustness variable on the Switch. This variable specifies how susceptible the subnet is to lost packets.	C	13
<code>ip igmp query-interval</code>	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
<code>ip igmp query-max-response-time <1-25></code>	Sets the maximum time that the router waits for a response to a general query message.	C	13
<code>ip igmp last-member-query-interval <1-25></code>	Sets the amount of time in seconds that the router waits for a response to a group specific query message.	C	13
<code>no ip igmp</code>	Disables IP IGMP in this routing domain.	C	13
<code>show ip igmp group</code>	Displays the multicast groups learned by IGMP.	E	3
<code>show ip igmp interface</code>	Displays the IGMP status information per interface.	E	3
<code>show ip igmp multicast</code>	Displays the multicast traffic information.	E	3
<code>show ip igmp timer</code>	Displays the IGMP timer settings.	E	3
<code>show router igmp</code>	Displays global IGMP settings.	E	3

Table 66 IPMC Command Summary

COMMAND	DESCRIPTION	M	P
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s).	C	13
<code>ipmc egress-untag-vlan <vlan-id></code>	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
<code>no ipmc egress-untag-vlan</code>	Disables the ports from removing the VLAN tags from outgoing IP multicast packets.	C	13

26.3 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
```


IGMP Snooping Commands

Use these commands to configure IGMP snooping on the Switch.

27.1 Command Summary

The following section lists the commands for this feature.

Table 67 igmp-flush Command Summary

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

Table 68 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 port(s).	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 VLAN(s)	E	3
igmp-snooping	Enables IGMP snooping.	C	13
no igmp-snooping	Disables IGMP snooping.	C	13
igmp-snooping 8021p-priority <0-7>	Sets the 802.1p priority for outgoing igmp snooping packets.	C	13
no igmp-snooping 8021p-priority	Disables changing the priority of outgoing IGMP control packets.	C	13
igmp-snooping 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 address(es) in a profile. <i>name</i> : 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

Table 68 igmp-snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
igmp-snooping host-timeout <1-16711450>	Sets the host timeout value.	C	13
igmp-snooping leave-timeout <1-16711450>	Sets the leave timeout value	C	13
igmp-snooping 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 leave-proxy	Enables IGMP snooping leave-proxy mode. In this mode, the Switch sends a leave message with its MAC address to the multicast router/switch only when it receives the leave message from the last host in a multicast group.	C	13
no igmp-snooping leave-proxy	Disables IGMP snooping leave-proxy mode. In this mode, the Switch just snoops on and sends the multicast router/switch all IGMP leave messages without changing their source MAC addresses.	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
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 unknown-multicast-frame <drop flooding>	Sets how to treat traffic from unknown multicast groups.	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 VLAN(s), port(s) and/or multicast group(s).	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 68 igmp-snooping Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show igmp-snooping group interface port-channel <i><port-list></i>	Displays the multicast group(s) to which the specified port(s) belongs.	E	3
show igmp-snooping group interface port-channel <i><port-list></i> count	Displays the number of the multicast group(s) to which the specified port(s) belongs.	E	3
show igmp-snooping group vlan <i><vlan-list></i>	Displays the multicast group(s) for the specified multicast VLAN(s).	E	3
show igmp-snooping group vlan <i><vlan-list></i> count	Displays the number of the multicast group(s) for the specified multicast VLAN(s).	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 <i><port-list></i>	Displays the multicast statistics of the specified port(s).	E	3
show igmp-snooping statistics system	Displays the multicast statistics of the Switch.	E	3
show igmp-snooping statistics vlan <i><vlan-list></i>	Displays the multicast statistics of the specified multicast VLAN(s).	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 69 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 <i><auto fixed></i>	Specifies how the VLANs on which the Switch snoops IGMP packets are selected. auto: The Switch learns multicast group membership on any VLAN. See the User's Guide for the maximum number of VLANs the switch supports for IGMP snooping. The Switch drops any IGMP control messages on other VLANs after it reaches this maximum number (auto mode). fixed: The Switch only learns multicast group membership on specified VLAN(s). The Switch drops any IGMP control messages for any unspecified VLANs (fixed mode). See the User's Guide for the maximum number of VLANs the switch supports for IGMP snooping.	C	13
igmp-snooping vlan <i><vlan-id></i> [name <i><name></i>]	Specifies which VLANs to perform IGMP snooping on if the mode is fixed. Optionally, sets a name for the multicast VLAN. <i>name</i> : 1-32 printable characters; spaces are allowed if you put the string in double quotation marks (").	C	13
no igmp-snooping vlan <i><vlan-id></i>	Removes IGMP snooping configuration on the specified VLAN if the mode is fixed.	C	13

Table 70 interface igmp Command Summary

COMMAND	DESCRIPTION	M	P
show interfaces config <i><port-list></i> igmp-group-limited	Displays the group limits for IGMP snooping.	E	3
show interfaces config <i><port-list></i> igmp-immediate-leave	Displays the immediate leave settings for IGMP snooping.	E	3

Table 70 interface igmp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show interfaces config <port-list> igmp-query-mode	Displays the IGMP query mode for the specified port(s).	E	3
show interfaces config <port-list> igmp-snooping filtering	Displays the name(s) of the IGMP filtering profiles used for the specified port(s).	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 port(s) is allowed to join.	E	3
show interfaces config <port-list> igmp-snooping leave-mode	Displays the IGMP leave mode of the specified port(s).	E	3
show interfaces config <port-list> igmp-snooping query-mode	Displays the IGMP querier mode of the specified port(s).	E	3
interface port-channel <port-list>	Enters config-interface mode for the specified port(s).	C	13
igmp-snooping fast-leave-timeout <200-6348800>	Set the IGMP snooping fast leave timeout (in milliseconds) the Switch uses to update the forwarding table for the port(s). 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 port(s). If IGMP filtering is enabled on the Switch, the port(s) can only join the multicast groups in the specified profile.	C	13
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 report(s) 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
igmp-snooping leave-timeout <200-6348800>	Set the IGMP snooping normal leave timeout (in milliseconds) the Switch uses to update the forwarding table for the port(s). 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

Table 70 interface igmp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
igmp-snooping querier-mode <auto fixed edge>	Specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. fixed: The Switch always treats the port(s) as IGMP query port(s). Select this when you connect an IGMP multicast server to the port(s). auto: The Switch uses the port as an IGMP query port if the port receives IGMP query packets. edge: The Switch does not use the port as an IGMP query port. The Switch does not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.	C	13
no igmp-snooping filtering profile	Prohibits the port(s) 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
igmp-group-limited	Enables the group limiting feature for IGMP snooping. You must enable IGMP snooping as well.	C	13
igmp-group-limited number <number>	Sets the maximum number of multicast groups allowed. number: 0-255	C	13
no igmp-group-limited	Disables multicast group limits.	C	13
igmp-immediate-leave	Enables the immediate leave function for IGMP snooping. You must enable IGMP snooping as well.	C	13
no igmp-immediate-leave	Disables the immediate leave function for IGMP snooping.	C	13
igmp-querier-mode <auto fixed edge>	Specifies whether or not and under what conditions the port(s) is (are) IGMP query port(s). The Switch forwards IGMP join or leave packets to an IGMP query port, treating the port as being connected to an IGMP multicast router (or server). You must enable IGMP snooping as well. fixed: The Switch always treats the port(s) as IGMP query port(s). Select this when you connect an IGMP multicast server to the port(s). auto: The Switch uses the port as an IGMP query port if the port receives IGMP query packets. edge: The Switch does not use the port as an IGMP query port. The Switch does not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.	C	13

27.2 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.

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

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

```

sysname# configure
sysname(config)# igmp-snooping
sysname(config)# interface port-channel 1
sysname(config-interface)# igmp-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 71 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
```


IGMP Filtering Commands

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

28.1 Command Summary

The following section lists the commands for this feature.

Table 72 igmp-filtering Command Summary

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

28.2 Command Examples

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

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

Interface Commands

Use these commands to configure basic port settings.

29.1 Command Summary

The following section lists the commands for this feature.

Table 73 interface Command Summary

COMMAND	DESCRIPTION	M	P
<code>clear interface <port-num></code>	Clears all statistics for the specified port.	E	13
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s).	C	13
<code>bpdu-control</code> <code><peer tunnel discard network></code>	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
<code>cx4-length <0.5 1 3 5 10 15></code>	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
<code>flow-control</code>	Enables interface flow control. Flow control regulates transmissions to match the bandwidth of the receiving port.	C	13
<code>frame-type</code> <code><all tagged untagged></code>	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
<code>inactive</code>	Disables the specified port(s) on the Switch.	C	13
<code>intrusion-lock</code>	Enables intrusion lock on the port(s) and a port cannot be connected again after you disconnected the cable. Note: Intrusion lock is not available on a 10 Gigabit Ethernet port.	C	13
<code>name <port-name-string></code>	Sets a name for the port(s). <i>port-name-string</i> : up to 64 English keyboard characters	C	13

Table 73 interface Command Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>no flow-control</code>	Disables flow control on the port(s).	C	13
<code>no inactive</code>	Enables the port(s) on the Switch.	C	13
<code>no intrusion-lock</code>	Disables intrusion-lock on a port so that a port can be connected again after you disconnected the cable.	C	13
<code>pvid <1-4094></code>	The default PVID is VLAN 1 for all ports. Sets a PVID in the range 1 to 4094 for the specified interface.	C	13
<code>qos priority <0-7></code>	Sets the quality of service priority for an interface.	C	13
<code>speed-duplex <auto 10-half 10-full 100-half 100-full 1000-full></code>	Sets the duplex mode (half or full) and speed (10, 100 or 1000 Mbps) of the connection on the interface. Select auto (auto-negotiation) to let the specified port(s) negotiate with a peer to obtain the connection speed and duplex mode.	C	13
<code>no interface <port-num></code>	Resets the port counters for the specified port(s).	E	13
<code>show interfaces <port-list></code>	Displays the current interface status for the specified port(s).	E	3
<code>show interfaces config <port-list></code>	Displays current interface configuration for the specified port(s).	E	3

29.2 Command Examples

This example looks at the current status of port 1.

```

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

```

The following table describes the labels in this screen.

Table 74 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 or 1000M for 1000 Mbps) and the duplex (F for full duplex or H for half duplex). It also shows the cable type (Copper or Fiber). This field displays Down if the port is not connected to any device.
Status	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port

Table 74 show interfaces (continued)

LABEL	DESCRIPTION
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.
Error Packet The following fields display detailed information about packets received that were in error.	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
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.

Table 74 show interfaces (continued)

LABEL	DESCRIPTION
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

```


Interface Route-domain Mode

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

30.1 Command Summary

The following section lists the commands for this feature.

Table 75 Interface Route Domain Command Summary:

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

30.2 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)#
```


IP Commands

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



See [Chapter 71 on page 275](#) for static route commands.



See [Chapter 32 on page 137](#) for IP source binding commands.

31.1 Command Summary

The following section lists the commands for this feature.

Table 76 ip Command Summary

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

Table 77 tcp and udp Command Summary

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

Table 77 tcp and udp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show ip udp	Displays IP UDP information.	E	3
kick tcp <session id>	Disconnects the specified TCP session. <i>session id</i> : Display the session id by running the show ip tcp command. See Section 31.2 on page 134 for an example.	E	13

31.2 Command Examples

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

```

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

```

The following table describes the labels in this screen.

Table 78 show ip tcp

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

Table 78 show ip tcp (continued)

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

Table 78 show ip tcp (continued)

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

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

```

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

```

The following table describes the labels in this screen.

Table 79 show ip udp

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

IP Source Binding Commands

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

32.1 Command Summary

The following section lists the commands for this feature.

Table 80 ip source binding Command Summary

COMMAND	DESCRIPTION	M	P
show ip source binding [<i><mac-addr></i>] [...]	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 <i><port-list></i>	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 <i><vlan-list></i>	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 <i><mac-addr></i> vlan <i><vlan-id></i> <i><ip></i> [interface port-channel <i><interface-id></i>]	Creates a static binding for ARP inspection.	C	13
no ip source binding <i><mac-addr></i> vlan <i><vlan-id></i>	Removes the specified static binding.	C	13

32.2 Command Examples

This example shows the current binding table.

```

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

```

The following table describes the labels in this screen.

Table 81 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.

IPv6 Commands

33.1 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 3.4×10^{38} IP addresses. At the time of writing, the Switch supports the following features.

- Static address assignment (see [Section 33.1.1 on page 139](#)) and stateless autoconfiguration (see [Stateless Autoconfiguration on page 142](#))
- Neighbor Discovery Protocol (see [Neighbor Discovery Protocol \(NDP\) on page 144](#))
- Remote Management using SNMP, Telnet, HTTP and FTP services (see [Chapter 61 on page 245](#))
- ICMPv6 (see [ICMPv6 on page 143](#))
- IPv4/IPv6 dual stack; the Switch can run IPv4 and IPv6 at the same time.
- DHCPv6 client and relay (see [DHCPv6 on page 142](#))
- Multicast Listener Discovery (MLD) snooping and proxy (see [Multicast Listener Discovery on page 144](#))

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

33.1.1 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.

33.1.2 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. The link-local unicast address format is as follows.

Table 82 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 83 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 Adresse

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 84 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 servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 85 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 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.

MAC	00	:	13	:	49	:	12	:	34	:	56
EUI-64	02	:	13	:	49	:	FF	:	FE	:	12 : 34 : 56

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 don’t 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 ¹another 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.

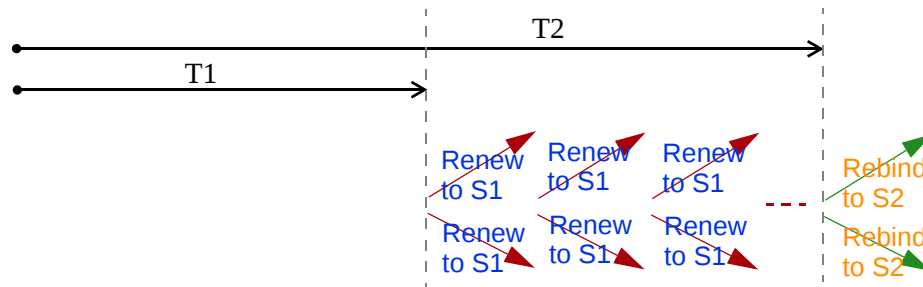
Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not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

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

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.



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 onlink, 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.

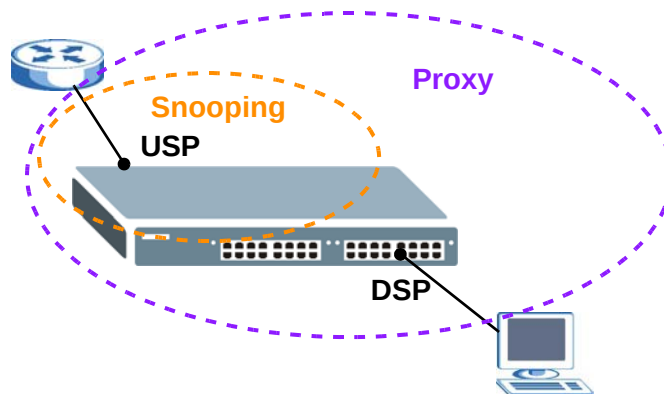
MLD Messages

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.

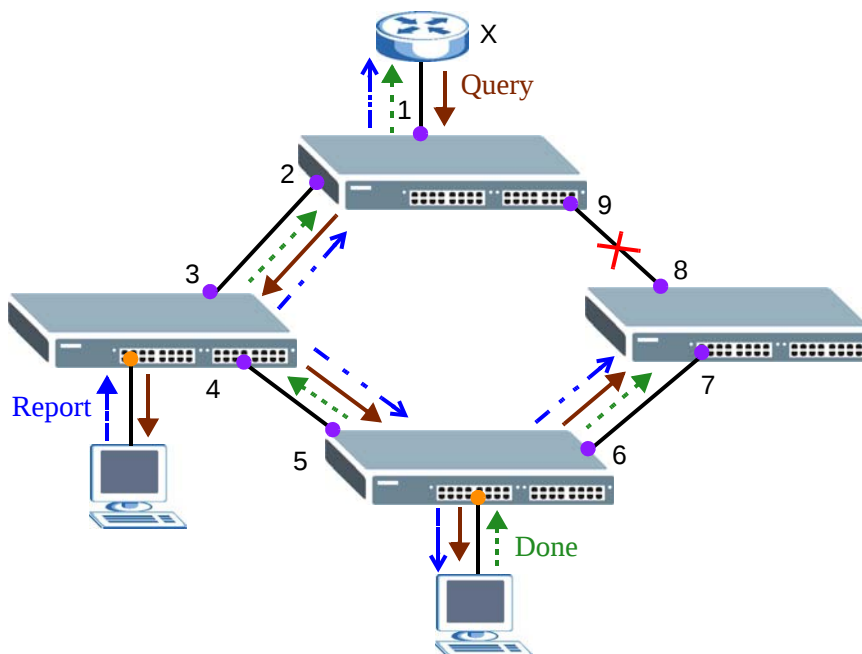


MLD Snooping-Proxy

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 via 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.



33.2 Command Summary

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

Table 86 ipv6 User-input Values

COMMAND	DESCRIPTION
<i>interface-type</i>	VLAN. The Switch supports only the VLAN interface type at the time of writing.
<i>interface-number</i>	A VLAN ID number.

The following section lists the commands for this feature.

Table 87 ipv6 address Command Summary

COMMAND	DESCRIPTION	M	P
<code>interface vlan <1-4094></code>	Enters config-route-domain mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
<code>ipv6</code>	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
<code>ipv6 address <ipv6-address>/<prefix></code>	Manually configures a static IPv6 global address for the VLAN.	C	13
<code>ipv6 address <ipv6-address>/<prefix> eui-64</code>	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

Table 87 ipv6 address Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 <iana>	Sets the Switch to get a non-temporary IP address from the DHCP server.	C	13
ipv6 address dhcp client <iana> [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
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
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 messag 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

Table 87 ipv6 address Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show ipv6 dhcp	Displays the Switch's DHCPv6 DUID.	E	3
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 <interface-type> <interface-number>	Displays IPv6 settings for a specified interface on the Switch.	E	3

Table 88 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
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 dhcp relay vlan <1-4094>	Disables DHCPv6 relay agent in the specified VLAN.	C	13
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 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 89 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> <[-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 90 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 port(s).	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 VLAN(s).	E	13
interface port-channel <port-list>	Enters config-interface mode for the specified port(s).	C	13
ipv6 mld snooping-proxy filtering group-limited	Enables multicast group limits for MLD snooping-proxy.	C	13

Table 90 ipv6 mld snooping-proxy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 mld snooping-proxy filtering group-limited number <i><number></i>	Sets the maximum number of the multicast groups the port(s) is allowed to join. <i>number</i> : 0 - 255	C	13
ipv6 mld snooping-proxy filtering profile <i><name></i>	Assigns the specified MLD filtering profile to the port(s). If MLD filtering is enabled on the Switch, the port(s) 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 port(s) and allows the port(s) 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 <i><0-7></i>	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 <i><name></i> start-address <i><ip></i> end-address <i><ip></i>	Adds an MLD filtering profile and sets the range of the multicast address(es).	C	13
ipv6 mld snooping-proxy vlan <i><vlan-id></i>	Enables MLD snooping-proxy on the specified VLAN.	C	13
ipv6 mld snooping-proxy vlan <i><vlan-id></i> downstream interface port-channel <i><port-list></i>	Specifies the downstream port(s) on the Switch. The port(s) 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 <i><vlan-id></i> downstream interface port-channel <i><port-list></i> fast-leave-timeout <i><2-16775168></i>	Sets the fast leave timeout (in milliseconds) for the specified downstream port(s). 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 <i><vlan-id></i> downstream interface port-channel <i><port-list></i> leave-timeout <i><2-16775168></i>	Set the MLD snooping normal leave timeout (in milliseconds) the Switch uses to update the forwarding table for the specified downstream port(s). 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 <i><vlan-id></i> downstream interface port-channel <i><port-list></i> mode <i><immediate normal fast></i>	Sets the leave mode for the specified downstream port(s) in a specified VLAN. This specifies whether Switch removes an MLD snooping membership entry (learned on a downstream port) immediately (<i>immediate</i>) or wait for an MLD report before the normal (<i>normal</i>) or fast (<i>fast</i>) leave timeout when an MLD leave message is received on this port from a host.	C	13
ipv6 mld snooping-proxy vlan <i><vlan-id></i> downstream query-interval <i><1000-31744000></i>	Sets the amount of time (in milliseconds) between general query messages sent by the downstream port.	C	13
ipv6 mld snooping-proxy vlan <i><vlan-id></i> downstream query-max-response-time <i><1000-25000></i>	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

Table 90 ipv6 mld snooping-proxy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ipv6 mld snooping-proxy vlan <vlan-id> upstream interface port- channel <port-list>	Specifies the upstream (host) port(s) on the Switch. The port(s) 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 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
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'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 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

Table 90 ipv6 mld snooping-proxy Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 address(es) 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 port(s) to not be a downstream port(s) for the specified VLAN.	C	13
no ipv6 mld snooping-proxy vlan <vlan-id> upstream interface port-channel <port-list>	Sets the specified port(s) to not be an upstream port(s) 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 port(s).	E	3
show interfaces config <port-list> mld snooping-proxy filtering profile	Displays the name of the filtering profile for the specified port(s).	E	3
show ipv6 mld snooping-proxy	Displays whether MLD snooping-proxy is enabled on the Switch and on which VLAN(s).	E	3
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 port(s).	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 VLAN(s).	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 91 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
ipv6 nd prefix <ipv6-prefix>/<prefix-length> [<valid-lifetime> [<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 via stateless address autoconfiguration remain preferred. no-autoconfig: indicates the hosts can not use this prefix for stateless address autoconfiguration. no-onlink: indicates this prefix can not 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 <1000-2147483647>	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

Table 91 ipv6 nd Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 (3000 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 (9000 seconds).	C	13
no ipv6 nd ra suppress	Enables the sending of router advertisements and responses to router solicitations on this interface.	C	13
no ipv6 nd reachable-time	Resets the reachable time of a neighbor to the default setting (60000 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 92 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

Table 92 ipv6 neighbor Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 IPv6 settings on the Switch and its neighbor devices.	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

33.3 Command Examples

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)# 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	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 93 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.
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)). Is it 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 (hh:mm:ss) an address can be used before it expires. If an address is manually configured, it displays permanent (never expires).

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 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#

```

33.4 Example - Enabling IPv6 on Windows XP/2003

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```

C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254

Tunnel adapter Teredo Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : fe80::5445:5245:444f%5
    Default Gateway . . . . . : 

Tunnel adapter Automatic Tunneling Pseudo-Interface:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : fe80::5efe:10.1.1.46%2
    Default Gateway . . . . . : 

```

IPv6 is installed and enabled by default in Windows Vista. Use the “ipconfig” command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

33.5 Example - HTTP Accessing the Switch Using IPv6

How you access the Switch using HTTP varies depending on the operating system (OS) and the type of browser you use and the type of address you want to access.



It's recommended to use Internet Explorer 7.0 or FireFox to access the Switch's web GUI.

Table 94 Specifying the Switch Address for HTTP Access

OS	DESTINATION	INTERNET EXPLORER 7.0	FIREFOX
Windows XP	A link-local address	Use <code>http://address</code> The address should be converted using the following procedure. 1. Use a dash “-” to replace each colon “:” in an IPv6 address. 2. Append the Ethernet interface identifier you want to use to connect to the Switch. But replace the percentage character “%” with “s”. 3. Append “.ipv6-literal.net” at the end. For example, the Switch uses an address <code>fe80::1234:5678</code> . The Ethernet interface identifier you want to use on your computer to access the Switch is <code>%4</code> . You have to type the following to access the Switch. <code>http://fe80--1234-5678-1s4.ipv6-literal.net</code> .	
	A global address	Use <code>http://[address]</code> For example, <code>http://[fe80--1234-5678-1]</code>	
Windows Vista	A link-local address		
	A global address		

This example shows you how to access the Switch using HTTP on Windows XP.

- 1 Make sure you have enabled IPv6 on your computer (see Section 33.4). Use the `ipconfig` command in the command prompt to check the IPv6 address on your computer. The example uses an interface with address “`fe80::2d0:59ff:feb8:103c`” to

access the Switch. So its Ethernet interface identifier is %4 and will be used later to make a ping.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254
```

- 2 Check the Switch IPv6 address(es) you want to ping. In this example, there are two IPv6 addresses in VLAN 1. One is a link-local address (fe80::219:cbff:fe00:1/64) and the other one is a global address (2001::1234/64).

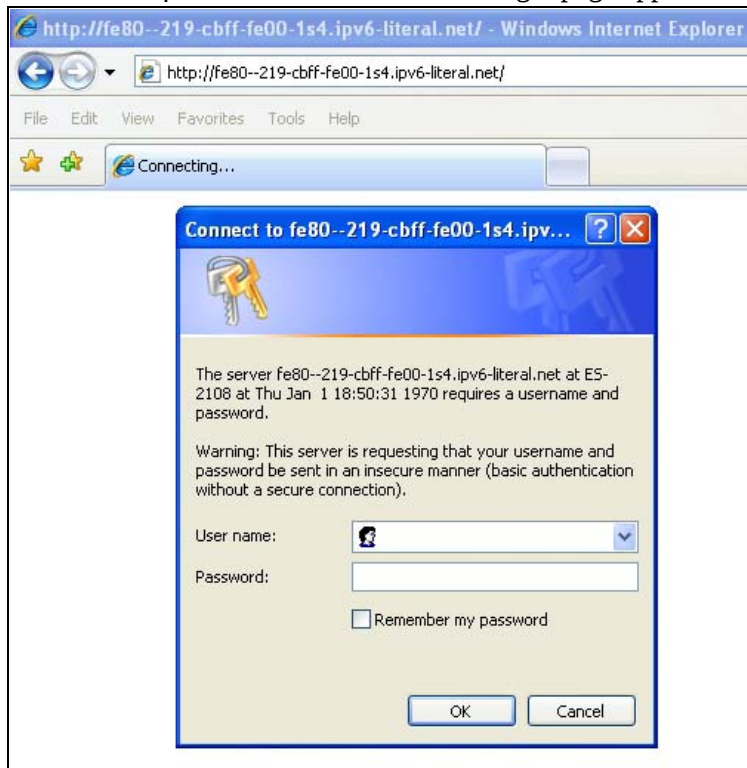
```
sysname# show ipv6

VLAN ID      : 1
IPv6 Status  : Enable

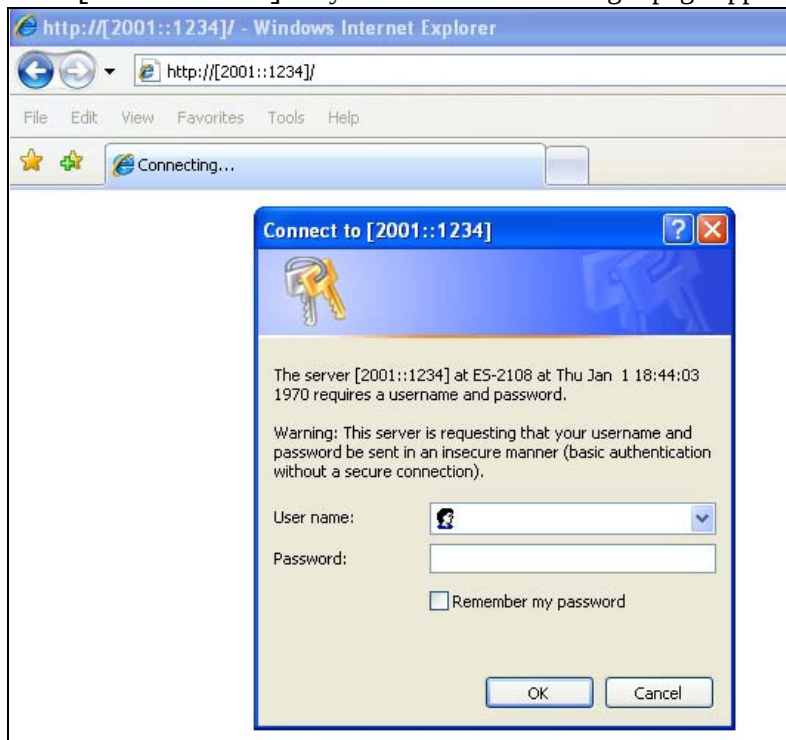
Origin      IP Address/PrefixLength      Status      Expire
-----
manual      fe80::219:cbff:fe00:1/64              preferred   permanent
manual      2001::1234/64                        preferred   permanent
```

- 3 In order to access the Switch through its link-local address, do the address conversion (See [Table 94 on page 159](#)).
 - 3a Use a dash “-” to replace each colon “:” in an IPv6 address. Then the address becomes:
fe80--219-cbff-fe00-1
 - 3b In the step 1, the Ethernet interface identifier you want to use to connect to the Switch is “%4”. Replace the percentage character “%” with “s” and then append it to the address. The address becomes:
fe80--219-cbff-fe00-1s4
 - 3c Append “.ipv6-literal.net” at the end. The address becomes:
fe80--219-cbff-fe00-1s4.ipv6-literal.net

Open an Internet Explorer 7.0 browser and type `http://fe80--219-cbff-fe00-1s4.ipv6-literal.net`. The login page appears.



- 4 Alternatively, you can use the global address to access the Switch. Type `http://[2001::1234]` on your browser and the login page appears.



Layer 2 Protocol Tunnel (L2PT) Commands

34.1 Command Summary

The following section lists the commands for this feature.

Table 95 l2pt Command Summary

COMMAND	DESCRIPTION	M	P
<code>clear l2protocol-tunnel</code>	Removes all layer 2 protocol tunneling counters.	E	13
<code>interface port-channel <port-list></code>	Enters config-interface mode for configuring the specified port(s).	C	13
<code>l2protocol-tunnel</code>	Enables layer 2 protocol tunneling for CDP (Cisco Discovery Protocol), STP (Spanning Tree Protocol) and VTP (VLAN Trunking Protocol) packets on the specified port(s).	C	13
<code>l2protocol-tunnel cdp</code>	Enables layer 2 protocol tunneling for CDP packets on the specified port(s).	C	13
<code>l2protocol-tunnel mode <access tunnel></code>	Sets the L2PT mode for the specified port(s) 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 port(s). Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) 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 service(s) is not enabled on an access port, the protocol packets are dropped.	C	13
<code>l2protocol-tunnel point-to-point</code>	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 port(s).	C	13
<code>l2protocol-tunnel point-to-point lacp</code>	Enables point-to-point layer 2 protocol tunneling for LACP packets on the specified port(s).	C	13
<code>l2protocol-tunnel point-to-point pagp</code>	Enables point-to-point layer 2 protocol tunneling for PAGP packets on the specified port(s).	C	13

Table 95 l2pt Command Summary (continued)

COMMAND	DESCRIPTION	M	P
l2protocol-tunnel point-to-point udld	Enables point-to-point layer 2 protocol tunneling for UDLD packets on the specified port(s).	C	13
l2protocol-tunnel stp	Enables layer 2 protocol tunneling for STP packets on the specified port(s).	C	13
l2protocol-tunnel vtp	Enables layer 2 protocol tunneling for CDP packets on the specified port(s).	C	13
no l2protocol-tunnel	Disables layer 2 protocol tunneling for CDP, VTP and STP packets on the specified port(s).	C	13
no l2protocol-tunnel cdp	Disables layer 2 protocol tunneling for CDP packets on the specified port(s).	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 port(s).	C	13
no l2protocol-tunnel point-to-point lacp	Disables point-to-point layer 2 protocol tunneling for LACP packets on the specified port(s).	C	13
no l2protocol-tunnel point-to-point pagp	Disables point-to-point layer 2 protocol tunneling for PAGP packets on the specified port(s).	C	13
no l2protocol-tunnel point-to-point udld	Enables point-to-point layer 2 protocol tunneling for UDLD packets on the specified port(s).	C	13
no l2protocol-tunnel stp	Disables layer 2 protocol tunneling for STP packets on the specified port(s).	C	13
no l2protocol-tunnel vtp	Disables layer 2 protocol tunneling for VTP packets on the specified port(s).	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 port(s).	E	13

34.2 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 Counter	Decapsulation Counter	Drop Counter
3	cdp	Enable	0	0	0
	stp	Enable	1280	2548	0
	vtp	Enable	0	0	0
	lacp	Disable	0	0	0
	pagp	Disable	0	0	0
	udld	Disable	0	0	0

```
sysname#
```


Link Layer Discovery Protocol (LLDP) Commands

35.1 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.

35.2 Command Summary

The following section lists the commands for this feature.

Table 96 lldp Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <port-list>	Enters config-interface mode for configuring the specified port(s).	C	13
lldp admin-status <tx-only rx-only tx-rx>	Sets LLDP operating mode. tx-only: the port(s) can only send LLDP packets. rx-only: the port(s) can only receive LLDP packets. tx-rx: the port(s) can send or receive LLDP packets.	C	13
lldp basic-tlv management-address	Enables the sending of Management Address TLVs on the port(s).	C	13
lldp basic-tlv port-description	Enables the sending of Port Description TLVs on the port(s).	C	13
lldp basic-tlv system-capabilities	Enables the sending of System Capabilities TLVs on the port(s).	C	13
lldp basic-tlv system-description	Enables the sending of System Description TLVs on the port(s).	C	13
lldp basic-tlv system-name	Enables the sending of System Name TLVs on the port(s).	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
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 port(s).	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 port(s).	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 via a media dependent interface (MDI) on the port(s).	C	13
no lldp admin-status	Sets the port(s) to not send or receive LLDP packets.	C	13
no lldp basic-tlv management-address	Disables the sending of Management Address TLVs on the port(s).	C	13
no lldp basic-tlv port-description	Disables the sending of Port Description TLVs on the port(s).	C	13
no lldp basic-tlv system-capabilities	Disables the sending of System Capabilities TLVs on the port(s).	C	13
no lldp basic-tlv system-description	Disables the sending of System Description TLVs on the port(s).	C	13

Table 96 lldp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no lldp basic-tlv system-name	Disables the sending of System Name TLVs on the port(s).	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 port(s).	C	13
no lldp org-specific-tlv dot1 port-vlan-id	Disables the sending of IEEE 802.1 Port VLAN ID TLVs on the port(s).	C	13
no lldp org-specific-tlv dot3 link-aggregation	Disables the sending of IEEE 802.3 Link Aggregation TLVs on the port(s).	C	13
no lldp org-specific-tlv dot3 mac-phy	Disables the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the port(s).	C	13
no lldp org-specific-tlv dot3 max-frame-size	Disables the sending of IEEE 802.3 Maximum Frame Size TLVs on the port(s).	C	13
no lldp org-specific-tlv dot3 power-via-mdi	Disables the sending of IEEE 802.3 Power via MDI TLVs on the port(s).	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	13
show lldp config interface port-channel <port-list>	Displays the LLDP settings on the specified port(s).	E	13
show lldp info local	Displays the Switch's device information.	E	13
show lldp info local interface port-channel <port-list>	Displays the LLDP information for the specified port(s).	E	13
show lldp info remote	Displays the device information from the neighboring devices.	E	13
show lldp info remote interface port-channel <port-list>	Displays the neighboring device information received on the specified port(s).	E	13
show lldp statistic	Displays LLDP statistics on the Switch.	E	13

Table 96 lldp Command Summary (continued)

COMMAND	DESCRIPTION	M	P
show lldp statistic interface port-channel <port-list>	Displays LLDP statistics of the specified port(s).	E	13
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 port(s).	E	13

35.3 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#

```

Load Sharing Commands

36.1 Load Sharing Overview

The Switch learns the next-hop(s) using ARP and determines routing path(s) 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.

36.2 Command Summary

The following section lists the commands for this feature.

Table 97 load-sharing Command Summary

COMMAND	DESCRIPTION	M	P
<code>ip load-sharing</code>	Enables load sharing on the Switch.	C	13
<code>ip load-sharing <sip sip-dip></code>	Sets the criteria the Switch uses to determine the routing path for a packe. 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
<code>ip load-sharing aging-time <0-86400></code>	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
<code>ip load-sharing discover-time <0-86400></code>	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
<code>no ip load-sharing</code>	Disables load sharing on the Switch.	C	13

36.3 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)#
```

Logging Commands

Use these commands to manage system logs.

37.1 Command Summary

The following section lists the commands for this feature.

Table 98 logging Command Summary

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

37.2 Command Examples

This example displays the system logs.

```

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

```


Login Account Commands

Use these commands to configure login accounts on the Switch.

38.1 Password Encryption

See [Section 50.1 on page 211](#) for information on this feature.

38.2 Command Summary

The following section lists the commands for this feature.

Table 99 logins Command Summary

COMMAND	DESCRIPTION	M	P
show logins	Displays login account information.	E	3
logins username <name> password <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. <i>name</i> : 1-32 alphanumeric characters. <i>password</i> : 1-32 alphanumeric characters.	C	14
logins username <name> password cipher <password> privilege <0-14>	Creates account with the specified user name and sets the cipher password and privilege. This is used for password encryption. The privilege level is applied the next time the user logs in. <i>name</i> : 1-32 alphanumeric characters. <i>password</i> : 32 alphanumeric characters.	C	14
no logins username <name>	Removes the specified account.	C	14

38.3 Command Examples

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

```
sysname# configure
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

Loopguard Commands

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

39.1 Command Summary

The following section lists the commands for this feature.

Table 100 loopguard Command Summary

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

39.2 Command Examples

This example enables loopguard on ports 1-3.

```

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

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

```

The following table describes the labels in this screen.

Table 101 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.

MAC Address Commands

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

40.1 Command Summary

The following section lists the commands for this feature.

Table 102 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. <i>sort</i> : MAC, VID, or PORT.	E	3
show mac address-table count	Displays the total number of MAC addresses in the MAC address table.	E	3
show mac address-table port <port-list> [<sort>]	Displays the MAC address table for the specified port(s). Sorted by MAC, Port or VID. <i>sort</i> : MAC, VID, or PORT.	E	3
show mac address-table static	Displays the static MAC address table.	E	3
show mac address-table vlan <vlan-list> [<sort>]	Displays the MAC address table for the specified VLAN(s). Optionally, sorted by MAC, Port or VID. <i>sort</i> : MAC, VID, or PORT.	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.	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 port(s) 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 VLAN(s) 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

Table 102 mac, mac-aging-time, and mac-flush Command Summary (continued)

COMMAND	DESCRIPTION	M	P
mac-transfer dynamic-to-forward interface port-channel <port-list>	Displays and changes all MAC addresses dynamically learned on the specified port(s) 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 VLAN(s) into static MAC addresses.	C	13

40.2 Command Examples

This example shows the current MAC address table.

```

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

```

The following table describes the labels in this screen.

Table 103 show mac address-table

LABEL	DESCRIPTION
Port	This is the port from which the above MAC address was learned. Drop: The entry is created from a filtering rule.
VLAN ID	This is the VLAN group to which this frame belongs.
MAC Address	This is the MAC address of the device from which this frame came.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered using mac-forward commands, see Chapter 43 on page 185).

MAC Authentication Commands

Use these commands to configure MAC authentication on the Switch.

41.1 MAC Authentication Overview

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



You also need to configure a RADIUS server (see [Chapter 60 on page 243](#)).

See also [Chapter 25 on page 107](#) for IEEE 802.1x port authentication commands and [Chapter 54 on page 223](#) for port security commands.

41.2 Command Summary

The following section lists the commands for this feature.

Table 104 mac-authentication Command Summary

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

Table 104 mac-authentication Command Summary (continued)

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

41.3 Command Examples

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

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

MAC Filter Commands

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



Use the running configuration commands to look at the current MAC filter settings. See [Chapter 64 on page 255](#).



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 42.2 on page 184](#) and [Section 42.3 on page 184](#) for examples.

42.1 Command Summary

The following section lists the commands for this feature.

Table 105 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. <i>name</i> : 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. <i>name</i> : 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

42.2 Command Example

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

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

42.3 Command Example: Filter Source

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

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

MAC Forward Commands

Use these commands to configure static MAC address forwarding.



Use the mac commands to look at the current mac - forward settings. See [Chapter 40 on page 179](#).

43.1 Command Summary

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

Table 106 mac-forward User-input Values

COMMAND	DESCRIPTION
<i>name</i>	1-32 alphanumeric characters

The following section lists the commands for this feature.

Table 107 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

Mirror Commands

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.



Use the running configuration commands to look at the current mirror settings. See [Chapter 64 on page 255](#).



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

44.1 Command Summary

The following section lists the commands for this feature.

Table 108 mirror Command Summary

COMMAND	DESCRIPTION	M	P
<code>mirror-port</code>	Enables port mirroring on the Switch.	C	13
<code>mirror-port <port-num></code>	Specifies the monitor port (the port to which traffic flow is copied) for port mirroring.	C	13
<code>no mirror-port</code>	Disables port mirroring on the Switch.	C	13
<code>no mirror-port <port-num></code>	Removes the specified monitor port. <i>port-num</i> : 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
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s). <i>port-list</i> : 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 desh (-) to indicates a range of ports. For example, "3/11,4/5" or "3/7-3/9".	C	13
<code>mirror</code>	Enables port mirroring in the interface.	C	13

Table 108 mirror Command Summary (continued)

COMMAND	DESCRIPTION	M	P
mirror dir <ingress egress both>	Enables port mirroring for incoming (ingress), outgoing (egress) or both incoming and outgoing (both) traffic.	C	13
no mirror	Disables port mirroring on the port(s).	C	13

Table 109 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
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

44.2 Command Examples

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

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

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:
```


MRSTP Commands

Use these commands to configure MRSTP on the Switch.

45.1 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 68 on page 267](#) for information on RSTP commands and [Chapter 46 on page 193](#) for information on MSTP commands.

45.2 Command Summary

The following section lists the commands for this feature.

Table 110 Command Summary: mrstp

COMMAND	DESCRIPTION	M	P
show mrstp <tree-index>	Displays multiple rapid spanning tree configuration for the specified tree. <i>tree-index</i> : 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
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

Table 110 Command Summary: mrstp

COMMAND	DESCRIPTION	M	P
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 <1-65535>	Sets a path cost to the specified ports.	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> 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 port(s).	C	13

45.3 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

```

MSTP Commands

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

46.1 Command Summary

The following section lists the commands for this feature.

Table 111 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. <i>name</i> : 1-32 printable characters	C	13
mstp revision <0-65535>	Sets the revision number for this MST Region configuration.	C	13
mstp hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	Sets Hello Time, Maximum Age and Forward Delay. hello-time: The time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. maximum-age: The maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. forward-delay: The maximum time (in seconds) the Switch will wait before changing states.	C	13
mstp max-hop <1-255>	Sets the maximum hop value before BPDUs are discarded in the MST Region.	C	13
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

Table 112 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 MST 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
mstp instance <number> interface port-channel <port-list> path-cost <1-65535>	Specifies the cost of transmitting a frame to a LAN through the port(s). It is recommended you assign it according to the speed of the bridge.	C	13
mstp instance <number> interface port-channel <port-list> priority <1-255>	Sets the priority for the specified ports. Priority decides which port should be disabled when more than one port forms a loop in a Switch. Ports with a higher priority numeric value are disabled first.	C	13

46.2 Command Examples

This example shows the current MSTP configuration.

```

sysname# show mstp
(a)BridgeMaxAge:           20      (seconds)
(b)BridgeHelloTime:        2       (seconds)
(c)BridgeForwardDelay:     15      (seconds)
(d)BridgeMaxHops:          128
(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 113 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 .
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.
vlangs 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 114 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.
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
```


Multiple Login Commands

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

47.1 Command Summary

The following section lists the commands for this feature.

Table 115 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

47.2 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 116 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.

MVR Commands

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

48.1 Command Summary

The following section lists the commands for this feature.

Table 117 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. <i>name</i> : 1-32 English keyboard characters	C	13
receiver-port <port-list>	Sets the receiver port(s).An MVR receiver port can only receive multicast traffic in a multicast VLAN.	C	13
no receiver-port <port-list>	Disables the receiver port(s).An MVR receiver port can only receive multicast traffic in a multicast VLAN.	C	13
source-port <port-list>	Sets the source port(s).An MVR source port can send and receive multicast traffic in a multicast VLAN.	C	13
no source-port <port-list>	Disables the source port(s).An MVR source port can send and receive multicast traffic in a multicast VLAN.	C	13
tagged <port-list>	Sets the port(s) to tag VLAN tags.	C	13
no tagged <port-list>	Sets the port(s) to untag VLAN tags.	C	13
group <name> start-address <ip> end-address <ip>	Sets the multicast group range for the MVR. <i>name</i> : 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

48.2 Command Examples

This example configures MVR in the following ways:

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

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

PART IV

Reference N-S

OSPF Commands (205)
Password Commands (211)
PoE Commands (213)
Policy Commands (217)
Policy Route Commands (221)
Port Security Commands (223)
Port-based VLAN Commands (225)
PPPoE IA Commands (227)
Private VLAN Commands (233)
Protocol-based VLAN Commands (237)
Queuing Commands (239)
RADIUS Commands (243)
Remote Management Commands (245)
RIP Commands (247)
Running Configuration Commands (255)
sFlow (257)
Smart Isolation Commands (259)
SNMP Server Commands (263)
STP and RSTP Commands (267)
SSH Commands (271)
Static Multicast Commands (273)
Static Route Commands (275)
Subnet-based VLAN Commands (279)

OSPF Commands

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

49.1 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.

49.2 Command Summary

The following section lists the commands for this feature.

Table 118 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 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
ip ospf authentication-same-aa	Sets the same OSPF authentication settings in the routing domain as the associated area.	C	13

Table 118 OSPF Command Summary (continued)

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

Table 118 OSPF Command Summary (continued)

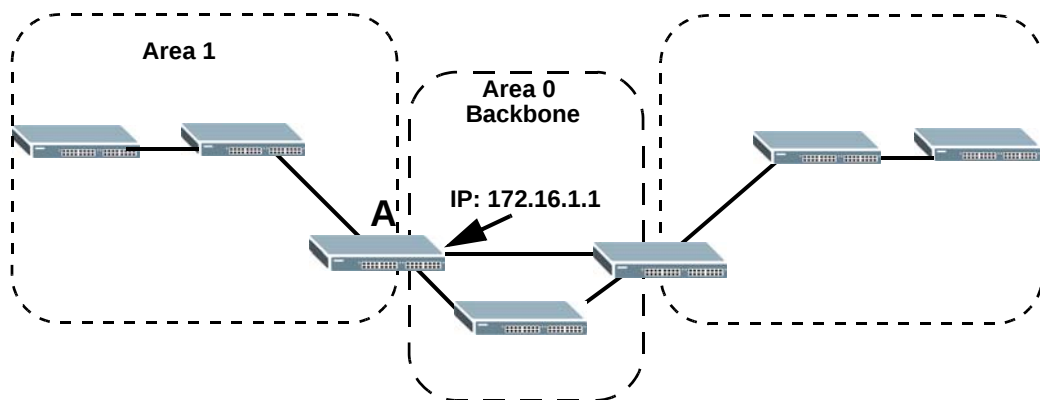
COMMAND	DESCRIPTION	M	P
no area <area-id> virtual-link <router-id> authentication-key	Resets the authentication settings on this virtual link.	C	13
area <area-id> virtual-link <router-ID> authentication-same-as-area	Sets the virtual link to use the same authentication method as the area.	C	13
no area <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
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 <0-16777214>	Sets the Switch to learn RIP routing information which will use the specified metric information.	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

Table 118 OSPF Command Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>redistribute static metric-type <1 2> metric <0-16777214></code>	Sets the Switch to learn static routing information which will use the specified metric information.	C	13
<code>redistribute static</code>	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
<code>no redistribute static</code>	Sets the Switch not to learn static routing information.	C	13
<code>passive-iface <ip-addr/bits></code>	Sets the interface to be passive. A passive interface does not send or receive OSPF traffic.	C	13
<code>no passive-iface <ip-addr/bits></code>	Sets the interface to not be passive.	C	13
<code>summary-address <ip-address> <mask></code>	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
<code>no summary-address <ip-address> <mask></code>	Removes a summary address.	C	13
<code>show router ospf summary-address</code>	Displays all summary addresses on the Switch.	E	3
<code>no router ospf</code>	Disables OSPF on the Switch.	C	13

49.3 Command Examples

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

Figure 7 OSPF Network Example

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

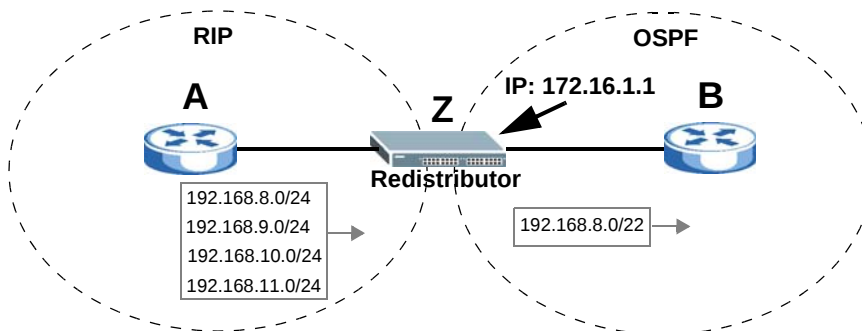
```
sysname(config)# router ospf 172.16.1.1
sysname(config-ospf)# area 0.0.0.0
sysname(config-ospf)# area 0.0.0.0 authentication
sysname(config-ospf)# area 0.0.0.0 name backbone
sysname(config-ospf)# network 172.16.1.1/24 area 0.0.0.0
sysname# show router ospf area
index:1      active:Y      name:backbone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

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

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

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 8 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  0x800000001  0x02f6  E1  192.168.8.0/24
192.168.9.0    192.168.2.2    618  0x800000001  0xf601  E1  192.168.9.0/24
192.168.10.0   192.168.2.2    618  0x800000001  0xeb0b  E1  192.168.10.0/24
192.168.11.0   192.168.2.2    618  0x800000001  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, 00001011 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 4 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   0x800000001  0xf209  E1  192.168.8.0/22

```

Password Commands

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

50.1 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.

50.2 Command Summary

The following section lists the commands for this feature.

Table 119 password Command Summary

COMMAND	DESCRIPTION	M	P
admin-password <pw-string> <confirm-string>	Changes the administrator password. <i>pw-string</i> : 1-32 alphanumeric characters <i>confirm-string</i> : 1-32 alphanumeric characters	C	14
admin-password <pw-string>	Changes the administrator password. <i>pw-string</i> : 1-32 alphanumeric characters	C	14
admin-password cipher <pw-string>	Sets the administrator cipher password, which is used in administrator password encryption. <i>pw-string</i> : 32 alphanumeric characters	C	14
password <password> [privilege <0-14>]	Changes the password for the highest privilege level or, optionally, the specified privilege. <i>password</i> : 1-32 alphanumeric characters	C	14
password cipher <pw-string> [privilege <0-14>]	Changes the password cipher for the highest privilege level or, optionally, the specified privilege. This is used in password encryption. <i>password</i> : 32 alphanumeric characters	C	14
no password privilege <0-14>	Clears the password for the specified privilege level and prevents users from entering the specified privilege level.	C	14
password encryption	Sets all password setting encryption.	C	14
no password encryption	Disables password encryption. The encrypted password will not be changed back to plain text.	C	14

50.3 Command Examples

See [Section 2.1.3.2 on page 18](#).

PoE Commands

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

51.1 Command Summary

The following section lists the commands for this feature.

Table 120 pwr Command Summary

COMMAND	DESCRIPTION	M	P
show pwr	Displays information about port power consumption and Power over Ethernet (PoE). Only available on models with the PoE feature.	E	3
show poe-status	This command is available for PoE models only. Displays information about Power over Ethernet (PoE) availability and usage.	E	0
pwr interface <port-list>	Enables PoE (Power over Ethernet) on the specified port(s).	C	13
pwr interface <port-list> priority <critical high low>	Sets the PD priority on a port to allow the Switch to allocate power to higher priority ports when the remaining power is less than the consumed power. critical > high > low Note: Available for non-full power models only.	C	13
no pwr interface <port-list>	Disables PoE (Power over Ethernet) on the specified port(s).	C	13
pwr mibtrap	Enables PoE MIB traps on the Switch. Traps are initiated when the usage reaches the limit set by the pwr usagethreshold command.	C	13
no pwr mibtrap	Disables PoE MIB traps on the Switch.	C	13
pwr usagethreshold <1-99>	Sets the percentage of power usage which initiates MIB traps.	C	13
pwr mode <classification consumption>	Set the power management mode. - Classification - Reserve the maximum power to each PD according to the priority level. - Consumption - Reserve the consuming power to each PD.	C	13

51.2 Command Examples

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

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

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

```
GS2200# sh pwr
PoE Mode : Classification mode
Total Power:220.0(W)
Consuming Power:0.0(W)
Allocated Power:0.0 (W)
Remaining Power:220.0(W)
Averaged Junction Temperature: 38 (c), 98 (f).
Port State PD Class Priority Consumption (mW) MaxPower(mW)
-----
1 Enable off 0 Low 0 0
2 Enable off 0 Low 0 0
3 Enable off 0 Low 0 0
4 Enable off 0 Low 0 0
5 Enable off 0 Low 0 0
6 Enable off 0 Low 0 0
7 Enable off 0 Low 0 0
8 Enable off 0 Low 0 0
9 Enable off 0 Low 0 0
10 Enable off 0 Low 0 0
11 Enable off 0 Low 0 0
12 Enable off 0 Low 0 0
13 Enable off 0 Low 0 0
14 Enable off 0 Low 0 0
15 Enable off 0 Low 0 0
16 Enable off 0 Low 0 0
17 Enable off 0 Low 0 0
18 Enable off 0 Low 0 0
19 Enable off 0 Low 0 0
20 Enable off 0 Low 0 0
21 Enable off 0 Low 0 0
22 Enable off 0 Low 0 0
23 Enable off 0 Low 0 0
24 Enable off 0 Low 0 0
```

The following table describes the labels in this screen.

Table 121 show pwr

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

Policy Commands

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



Configure classifiers before you configure policies. See [Chapter 11 on page 59](#) for more information on classifiers.

52.1 Command Summary

The following section lists the commands for this feature.

Table 122 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 122 policy Command Summary

COMMAND	DESCRIPTION	M	P
<pre>policy <name> classifier <classifier-list> <[vlan <vlan- id>][egress-port <port- num>][priority <0-7>][dscp <0- 63>][tos <0-7>][bandwidth <bandwidth>][egress-mask <port- list>][outgoing-packet-format <tagged untagged>][out-of- profile-dscp <0-63>][forward- action <drop forward egressmask>][queu e-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]></pre>	Configures a policy with the specified name. <i>name</i>: 32 alphanumeric characters Specifies which classifiers this policy applies to. <i>classifier-list</i>: names of classifiers separated by commas. Specifies the parameters related to the actions: egress-port: an outbound port number priority: IEEE 802.1p priority field bandwidth: bandwidth limit in Kbps, actions can be assigned to packets which exceed the bandwidth limit (out-or-profile). out-of-profile-dscp: sets a DSCP number, if you want to replace or remark the DSCP number for out-of-profile traffic. Specifies the actions for this policy: - queue-action: tells the Switch to: - set the IEEE 802.1p priority you specified in the priority parameter (prio-set) - 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 122 policy Command Summary

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. <i>name</i> : 32 alphanumeric characters	C	13
	Specifies which classifiers this policy applies to. <i>classifier-list</i> : 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

52.2 Command Examples

This example creates a policy (**highPriority**) for the traffic flow identified via classifier **VLAN3** (see the classifier example in [Chapter 11 on page 59](#)). 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 via classifier **Class1** (see the classifier example in [Chapter 11 on page 59](#)). 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#
```

Policy Route Commands

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.



Configure layer-3 classifiers before you configure policy routing. See [Chapter 11 on page 59](#) for more information on classifiers.

53.1 Command Summary

The following section lists the commands for this feature.

Table 123 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. <i>name</i> : 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 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
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

53.2 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#
```

Port Security Commands

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



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

54.1 Command Summary

The following section lists the commands for this feature.

Table 124 port-security Command Summary

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

Table 124 port-security Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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

54.2 Command Examples

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

```

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

```

Port-based VLAN Commands

Use these commands to configure port-based VLAN.



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

55.1 Command Summary

The following section lists the commands for this feature.

Table 125 egress Command Summary

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

55.2 Command Examples

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

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


PPPoE IA Commands

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.

56.1 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.

56.1.1 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 port(s).



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 port(s).

- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

56.2 Command Summary

The following section lists the commands for this feature.

Table 126 PPPoE Intermediate Agent Command Summary

COMMAND	DESCRIPTION	M	P
<code>clear pppoe intermediate-agent statistics</code>	Removes all statistics records of PPPoE packets on the Switch.	E	13
<code>clear pppoe intermediate-agent statistics vlan <vlan-list></code>	Removes statistics records of PPPoE packets for the specified VLAN(s).	E	13
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s).	C	13
<code>pppoe intermediate-agent trust</code>	Sets the specified port(s) as PPPoE IA trusted port(s).	C	13
<code>pppoe intermediate-agent format-type circuit-id string <string></code>	Specify a string the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. <i>string</i> : up to 63 ASCII characters	C	13
<code>pppoe intermediate-agent format-type remote-id string <string></code>	Specify a string the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. <i>string</i> : up to 63 ASCII characters	C	13
<code>pppoe intermediate-agent vlan <vlan-id> format-type circuit-id string <string></code>	Specify 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
<code>pppoe intermediate-agent vlan <vlan-id> format-type remote-id string <string></code>	Specify 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
<code>no pppoe intermediate-agent trust</code>	Sets the specified port(s) PPPoE IA untrusted port(s).	C	13
<code>no pppoe intermediate-agent format-type circuit-id</code>	Disables the PPPoE IA Circuit ID settings for the specified port(s).	C	13
<code>no pppoe intermediate-agent format-type remote-id</code>	Disables the PPPoE IA Remote ID settings for the specified port(s).	C	13
<code>no pppoe intermediate-agent vlan <vlan-id> format-type circuit-id</code>	Disables the PPPoE IA Circuit ID settings for the specified port(s) on the specified VLAN(s).	C	13
<code>no pppoe intermediate-agent vlan <vlan-id> format-type remote-id</code>	Disables the PPPoE IA Remote ID settings for the specified port(s) on the specified VLAN(s).	C	13
<code>no pppoe intermediate-agent</code>	Disables PPPoE IA globally.	C	13
<code>no pppoe intermediate-agent vlan <vlan-list> remote-id</code>	Disables the PPPoE IA Remote ID settings for the specified VLAN(s).	C	13

Table 126 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 vlan <vlan-list>	Disables PPPoE IA for the specified VLAN(s).	C	13
no pppoe intermediate-agent vlan <vlan-list> circuit-id	Disables the PPPoE IA Circuit ID settings for the specified VLAN(s).	C	13
no pppoe intermediate-agent vlan <vlan-list> remote-id	Disables the PPPoE IA Remote ID settings for the specified VLAN(s).	C	13
pppoe intermediate-agent	Enables PPPoE Intermediate Agent (PPPoE IA) globally.	C	13
pppoe intermediate-agent format-type access-node-identifier string <string>	Sets the access-node-identifier string. <i>string</i> : 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 VV	13
pppoe intermediate-agent format-type identifier-string string <string> option <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. <i>string</i> : You can up to 63 printable characters. Spaces are allowed. option <sp sv pv spv>: 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 VLAN(s).	C	13
pppoe intermediate-agent vlan <vlan-list> circuit-id	Enables the PPPoE IA Circuit ID settings for the specified VLAN(s).	C	13
pppoe intermediate-agent vlan <vlan-list> remote-id	Enables the PPPoE IA Remote ID settings for the specified VLAN(s).	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 VLAN(s).	E	13

56.3 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 belong to the same 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
```

56.3.1 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 didn't 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 didn't assign the appended string for remote-id in example 1 and 2, it will carry the client's MAC address as default.

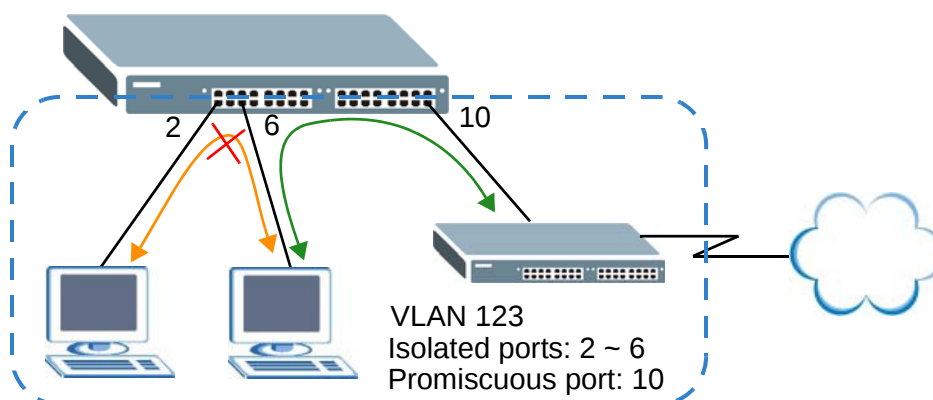
Private VLAN Commands

This chapter explains how to use commands to configure private VLANs on the Switch.

57.1 Private VLAN Overview

Private VLAN allows you to do port isolation within a VLAN in a simple way. In private VLAN, a promiscuous port can communicate with any port in the same VLAN. While an isolated port can communicate with the promiscuous port(s) only.

Figure 9 Private VLAN Example



If you change the VLAN settings, make sure you keep at least one port in the promiscuous port list for a VLAN with private VLAN enabled. Otherwise, this VLAN is blocked from the whole network.

57.2 Command Summary

The following section lists the commands for this feature.

Table 127 private-vlan Command Summary

COMMAND	DESCRIPTION	M	P
no private-vlan <vlan-id>	Removes the specified private VLAN rule.	C	13
no private-vlan <vlan-id> inactive	Enables the specified private VLAN rule.	C	13
private-vlan name <name> vlan <vlan-id> promiscuous-port <port-list>	Sets a private VLAN rule. You specify which port(s) in a VLAN is not isolated by adding it 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 name, VLAN ID and the promiscuous ports. You can enter individual ports separated by a comma or a range of ports by using a dash. For example, 1,3,5-8 indicates ports 1 and 3 and ports 5 through 8 are the promiscuous ports.	C	13
private-vlan name <name> vlan <vlan-id> promiscuous-port <port-list> inactive	Disables a private VLAN rule.	C	13
private-vlan name <name> vlan <vlan-id>	Sets a private VLAN rule for the specified VLAN. The Switch automatically adds all ports (except the uplink port(s)) 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
private-vlan name <name> vlan <vlan-id> inactive	Disables a private VLAN rule.	C	13
show private-vlan	Displays the settings and status of all private VLAN rules on the Switch.	E	3
show private-vlan <vlan-id>	Displays the settings and status of the specified private VLAN rule on the Switch.	E	3

57.3 Command Examples

This example sets a private VLAN 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 private VLAN rules configured on the Switch.

```

sysname# configure
sysname(config)# private-vlan name pvlan-123 vlan 123 promiscuous-port 7-8
sysname(config)# exit
sysname# show private-vlan
  Private VLAN: 123      Active: Yes
  Name      Promiscuous Port
  -----
  pvlan-123  7-8
sysname#

```

This example sets a private VLAN 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 private VLAN rules configured on the Switch.

```
sysname# configure
sysname(config)# private-vlan name pvlan-111 vlan 111
sysname(config)# exit
sysname# show private-vlan
  Private VLAN: 111    Active: Yes
  Name      Promiscuous Port
  -----
  pvlan-111  24
sysname#
```


Protocol-based VLAN Commands

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

58.1 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 72 on page 279](#) for subnet-based VLAN commands and [Chapter 78 on page 297](#) for VLAN commands.

58.2 Command Summary

The following section lists the commands for this feature.

Table 128 protocol-based-vlan Command Summary

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

Table 128 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. <i>name</i> - Use up to 32 alphanumeric characters. <i>ether-num</i> - if you don't 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. <i>priority</i> - 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

58.3 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#

```

Queuing Commands

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



Queuing method configuration differs across Switch models.

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

59.1 Queuing Overview

The following queuing algorithms are supported by ZyXEL Switches:



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

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



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

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

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

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

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

- **Weighted Round Robin Scheduling (WRR)** - services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is 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.

59.2 Command Summary: Port by Port Configuration

The following section lists the commands for this feature.

Table 129 Queuing Command Summary

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

Table 129 Queuing Command Summary (continued)

COMMAND	DESCRIPTION	M	P
ge-spq <q0 q1 ... q7>	Enables SPQ starting with the specified queue and subsequent higher queues on the Gigabit ports.	C	13
hybrid-spq lowest-queue <q0 q1 ... q7>	Enables SPQ starting with the specified queue and subsequent higher queues on the ports.	C	13
hybrid-spq <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

59.3 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

```

59.4 Command Summary: System-Wide Configuration

The following section lists the commands for this feature.

Table 130 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 4 queues.	C	13
spq	Sets the Switch to use Strictly Priority Queuing (SPQ).	C	13
wrr	Sets the Switch to use Weighted Round Robin (WRR).	C	13
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

59.5 Command Examples: System-Wide

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

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

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

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

RADIUS Commands

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

60.1 Command Summary

The following section lists the commands for this feature.

Table 131 radius-server Command Summary

COMMAND	DESCRIPTION	M	P
show radius-server	Displays RADIUS server settings.	E	3
radius-server host <index> <ip> [auth-port <socket-number>] [key <key-string>]	Specifies the IP address of the RADIUS authentication server. Optionally, sets the UDP port number and shared secret. <i>index</i> : 1 or 2. <i>key-string</i> : 1-32 alphanumeric characters.	C	14
radius-server mode <index- priority round-robin>	Specifies how the Switch decides which RADIUS server to select if you configure multiple servers. <i>index-priority</i> : 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. <i>round-robin</i> : 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. In <i>index-priority</i> mode, the timeout is divided by the number of servers you configure. For example, if you configure two servers and the timeout is 30 seconds, then the Switch waits 15 seconds for a response from each server.	C	14
no radius-server <index>	Resets the specified RADIUS server to its default values.	C	14

Table 132 radius-accounting Command Summary

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

Table 132 radius-accounting Command Summary (continued)

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

60.2 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
```

Remote Management Commands

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

61.1 Command Summary

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

Table 133 remote-management User-input Values

COMMAND	DESCRIPTION
<i>index</i>	1-4

The following section lists the commands for this feature.

Table 134 remote-management Command Summary

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

Table 135 service-control Command Summary

COMMAND	DESCRIPTION	M	P
show service-control	Displays service control settings.	E	3
service-control ftp	Allows FTP access to the Switch.	C	13
service-control ftp <socket-number>	Specifies the service port for the FTP service.	C	13

Table 135 service-control Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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). <i>timeout: 1-255</i>	C	13
no service-control http	Disables HTTP access to the Switch.	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
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>	Specifies the service port for the Telnet service.	C	13
no service-control telnet	Disables Telnet access to the Switch.	C	13

61.2 Command Examples

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

```

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

```

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

```

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

```

RIP Commands

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

62.1 RIP Overview

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

62.2 Command Summary

The following section lists the commands for this feature.

Table 136 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 136 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
no router rip	Disables RIP on the Switch.	C	13
interface route-domain <ip-address>/<mask-bits>	Enters the configuration mode for this routing domain.	C	13
ip rip direction <Outgoing Incoming Both None> version <v1 v2b v2m>	Sets the RIP direction and version in this routing domain.	C	13

62.3 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
```

63.1 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 via SNMP.

RMON groups contain detailed information about specific activities. The following table describes the four RMON groups that your Switch supports.

Table 137 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.

63.2 User Input Values

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

Table 138 rmon command user input values

USER INPUT	DESCRIPTION
<i>event-index</i>	This is an event's index number in the event table, between 1 and 65535.
<i>alarm-index</i>	This is an alarm's index number in the alarm table, between 1 and 65535.
<i>etherstats-index</i>	This is an entry's index number in the Ethernet statistics table, between 1 and 65535.
<i>historycontrol-index</i>	This is an entry's index number in the history control table, between 1 and 65535.
<i>owner</i>	This is a person's name who will handle the event, alarm, historycontrol, or Ethernet statistics entry.
<i>interface-id</i>	This is a port that the Switch will poll for data.

63.3 Command Summary

The following section lists the commands for this feature.

Table 139 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 63.3.2 on page 251 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

63.3.1 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

```

63.3.2 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 variable(s) 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>]

<i>interval-integer</i>	This is the time interval (in seconds) between data samplings.
<i>absolute delta</i>	This is the method of obtaining the sample value and calculating the value to be compared against the thresholds. • <i>absolute</i> - the sampling value of the selected variable will be compared directly with the thresholds. • <i>delta</i> - 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.
<i>startup-alarm</i>	Specify when the Switch should generate an alarm regarding to the rising and/or falling thresholds. • <i>risingAlarm</i> - the Switch generates an alarm if the sampling value (or calculated value) is greater than or equal to the rising threshold. • <i>fallingAlarm</i> - the Switch generates an alarm if the sampling value (or calculated value) is less than or equal to the falling threshold. • <i>risingOrFallingAlarm</i> - 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.
<i>rising-integer</i>	Specify an integer for the rising threshold. When a value that is greater or equal to this threshold, the Switch generates an alarm.
<i>rising-event-index</i>	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.
<i>falling-integer</i>	Specify an integer for the falling threshold. When a value that is smaller or equal to this threshold, the Switch generates an alarm.
<i>falling-event-index</i>	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.
<i>owner</i>	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 errored 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 63.3.1 on page 251](#))
- the falling threshold: 0
- which event's action should be taken for the falling alarm: 0 (see [Section 63.3.1 on page 251](#))
- 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#

```

63.3.3 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#

```

63.3.4 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#
```

Running Configuration Commands

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

64.1 Switch Configuration File

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

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

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



The Switch rejects configuration files with invalid or incomplete commands.

64.2 Command Summary

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

Table 140 running-config User-input Values

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

The following section lists the commands for this feature.

Table 141 running-config Command Summary

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

64.3 Command Examples

This example resets the Switch to the factory default settings.

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

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

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

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.

65.1 sFlow Overview

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.

65.2 Command Summary

The following section lists the commands for this feature.

Table 142 sflow Command Summary

COMMAND	DESCRIPTION	M	P
interface port-channel <port-list>	Enters config-interface mode for the specified port(s).	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

Table 142 sflow Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no sflow collector <ip-address>	Removes an sFlow collector entry.	C	13
sflow	Enables the sFlow agent on the Switch.	C	13
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

65.3 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
    ....

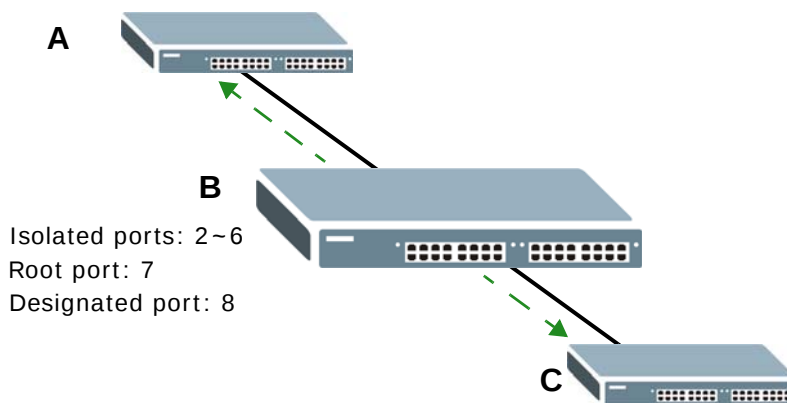
```

Smart Isolation Commands

This chapter explains how to use commands to configure smart isolation on the Switch.

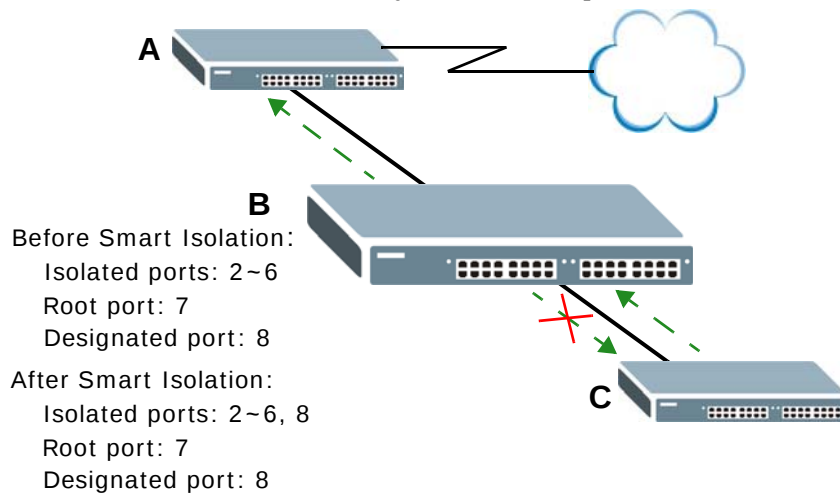
66.1 Smart Isolation Overview

To block traffic between two specific ports within the Switch, you can use port isolation or private VLAN (see [Chapter 57 on page 233](#) for more information). However, it does not work across multiple switches. For example, broadcast traffic from isolated ports on a switch (say **B**) can be forwarded to all ports on other switches (**A** and **C**), including the isolated ports.



Smart isolation allows you to prevent isolated ports on different switches from transmitting traffic to each other. After you enable RSTP/MRSTP and smart isolation on the Switch, the designated port(s) will be added to the isolated port list. In the following example, switch **A** is the root bridge. Switch **B**'s root port 7 connects to switch **A** and switch **B**'s designated port 8

connects to switch **C**. Traffic from isolated ports on switch **B** can only be sent through non-isolated port **1** or root port **7** to switch **A**. This prevents isolated ports on switch **B** sending traffic through designated port **8** to switch **C**. Traffic received on designated port **8** from switch **C** will not be forwarded to any other isolated ports on switch **B**.



You should enable RSTP or MRSTP before you can use smart isolation on the Switch. If the network topology changes, the Switch automatically updates the isolated port list with the latest designated port information.



The uplink port connected to the Internet should be the root port. Otherwise, with smart isolation enabled, the isolated ports cannot access the Internet.

66.2 Command Summary

The following section lists the commands for this feature.

Table 143 smart-isolation Command Summary

COMMAND	DESCRIPTION	M	P
no smart-isolation	Disables smart isolation on the Switch.	C	13
show smart-isolation	Enables smart isolation on the Switch.	E	3
smart-isolation	Displays the smart isolation status and information on the Switch.	C	13

66.3 Command Examples

This example enables smart isolation and displays smart isolation status and information on the Switch. You should have configured RSTP or MRSTP on the Switch in order to have smart isolation work by adding the designated port(s) to the isolated port list. You also have created VLAN 200 and configured a private VLAN rule for VLAN 200 to put ports 3, 4 and 5 in the isolated port list. In this example, the designated port 7 is added to the isolated port list after smart isolation is enabled.

```

sysname# configure
sysname(config)# spanning-tree mode rstp
sysname(config)# spanning-tree
sysname(config)# spanning-tree priority 32768
sysname(config)# spanning-tree 3-5, 7-8
sysname(config)# vlan 200
sysname(config-vlan)# fixed 3-5, 7-8
sysname(config-vlan)# untagged 3-5, 7-8
sysname(config-vlan)# exit
sysname(config)# private-vlan name pvlan-200 vlan 200 promiscuous-port 7-8
sysname(config)# smart-isolation
sysname(config)# exit
sysname# show smart-isolation
    smart isolation enable

Private VLAN:
  Original VLAN:
    VLAN 200
      isolated 3-5
      promiscuous 7-8

  Smart Isolated VLAN:
    VLAN 200
      isolated 3-5,7
      promiscuous 8

sysname#

```

The following table describes the labels in this screen.

Table 144 show smart-isolation

LABEL	DESCRIPTION
Port isolation	This section is available only when you have configured port isolation on the Switch. The following fields display the port isolation information before and after smart isolation is enabled.
original isolated ports	This field displays the isolated port list before smart isolation is enabled.
smart isolated ports	This field displays the isolated port list after smart isolation is enabled.
Private VLAN	This section is available only when you have configured private VLAN on the Switch. The following fields display the private VLAN information before and after smart isolation is enabled.

Table 144 show smart-isolation (continued)

LABEL	DESCRIPTION
Original VLAN	This section displays the VLAN ID and isolated and promiscuous port list before smart isolation is enabled
Smart Isolated VLAN	This section displays the VLAN ID and isolated and promiscuous port list after smart isolation is enabled

SNMP Server Commands

Use these commands to configure SNMP on the Switch.

67.1 Command Summary

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

Table 145 snmp-server User-input Values

COMMAND	DESCRIPTION
<i>property</i>	1-32 alphanumeric characters
<i>options</i>	aaa: authentication, accounting. interface: linkup, linkdown, autonegotiation, lldp, transceiver-ddm. ip: ping, traceroute. switch: stp, mactable, rmon, cfm. system: coldstart, warmstart, fanspeed, temperature, voltage, reset, timesync, intrusionlock, loopguard, poe.

The following section lists the commands for this feature.

Table 146 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. <i>system-contact</i> : 1-32 English keyboard characters; spaces are allowed. <i>system-location</i> : 1-32 English keyboard characters; spaces are allowed.	C	13
snmp-server version <v2c v3 v3v2c>	Sets the SNMP version to use for communication with the SNMP manager.	C	13
snmp-server get-community <property>	Sets the get community. Only for SNMPv2c or lower.	C	13
snmp-server set-community <property>	Sets the set community. Only for SNMPv2c or lower.	C	13
snmp-server trap-community <property>	Sets the trap community. Only for SNMPv2c or lower.	C	13

Table 146 snmp-server Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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
no snmp-server trap-destination <ip>	Deletes the specified SNMP manager.	C	13
snmp-server username <name> sec- level <noauth auth priv> [auth <md5 sha> auth-password <password>] [priv <des aes> priv-password <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. <i>name</i>: Enter the SNMP username. <i>noauth</i>: Use the username as the password string sent to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. <i>auth</i>: Implement an authentication algorithm for SNMP messages sent by this user. <i>priv</i>: Implement privacy settings and encryption for SNMP messages sent by this user. This is the highest security level. <i>auth-password</i>: Set the authentication password for SNMP messages sent by this user. <i>priv-password</i>: Set the privacy settings password for SNMP messages sent by this user. <i>group-name</i>: Set the View-based Access Control Model (VACM) group. Available group names are: <i>admin</i>: The user belongs to the admin group and has maximum access rights to the Switch. <i>readwrite</i>: The user can read and configure the Switch except for confidential options (such as user account and AAA configuration options.) <i>readonly</i>: The user can read but cannot make any configuration changes. 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 147 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

Table 147 snmp-server trap-destination enable traps Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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
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

67.2 Command Examples

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
```

STP and RSTP Commands

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

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

See [Chapter 45 on page 191](#) and [Chapter 46 on page 193](#) for more information on MRSTP and MSTP commands respectively. See also [Chapter 39 on page 177](#) for information on loopguard commands.

68.1 Command Summary

The following section lists the commands for this feature.

Table 148 spanning-tree Command Summary

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

Table 148 spanning-tree Command Summary (continued)

COMMAND	DESCRIPTION	M	P
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 <1-65535>	Specifies the cost of transmitting a frame to a LAN through the port(s). It is assigned according to the speed of the bridge.	C	13
spanning-tree <port-list> priority <0-255>	Sets the priority for the specified ports. Priority decides which port should be disabled when more than one port forms a loop in a Switch. Ports with a higher priority numeric value are disabled first.	C	13
spanning-tree help	Provides more information about the specified command.	C	13

68.2 Command Examples

This example configures STP in the following ways:

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

```

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

```

This example shows the current STP settings.

```

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

```

The following table describes the labels in this screen.

Table 149 show spanning-tree config

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

Table 149 show spanning-tree config (continued)

LABEL	DESCRIPTION
TransmissionLimit	This field displays the maximum number of BPDUs that can be transmitted in the interval specified by BridgeHelloTime .
ForceVersion	This field indicates whether BPDUs are RSTP (a value less than 3) or MSTP (a value greater than or equal to 3).

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
```

SSH Commands

Use these commands to configure SSH on the Switch.

69.1 Command Summary

The following section lists the commands for this feature.

Table 150 ssh Command Summary

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

69.2 Command Examples

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

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

This example shows the general SSH settings.

```

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

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

```

The following table describes the labels in this screen.

Table 151 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.

Static Multicast Commands

Use these commands to tell the Switch how to forward specific multicast frames to specific port(s). You can also configure which to do with unknown multicast frames using the `router igmp unknown-multicast-frame` command (see [Table 65 on page 111](#)).

70.1 Command Summary

The following section lists the commands for this feature.

Table 152 multicast-forward Command Summary

COMMAND	DESCRIPTION	M	P
<code>show mac address-table multicast</code>	Displays the multicast MAC address table.	E	3
<code>multicast-forward name <name> mac <mac-addr> vlan <vlan-id> inactive</code>	Creates a new static multicast forwarding rule. The rule name can be up to 32 printable ASCII characters. <i>mac-addr</i> : 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. <i>vlan-id</i> : A VLAN identification number. Note: Static multicast addresses do not age out.	C	13
<code>multicast-forward name <name> mac <mac-addr> vlan <vlan-id> interface port-channel <port-list></code>	Associates a static multicast forwarding rule with specified port(s) within a specified VLAN.	C	13
<code>no multicast-forward mac <mac-addr> vlan <vlan-id></code>	Removes a specified static multicast rule.	C	13
<code>no multicast-forward mac <mac-addr> vlan <vlan-id> inactive</code>	Activates a specified static multicast rule.	C	13

70.2 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
```

Static Route Commands

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

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

71.1 Command Summary

The following section lists the commands for this feature.

Table 153 ip route Command Summary

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

71.2 Command Examples

This example shows the current routing table.

```

sysname# show ip route
Dest          FF Len Device      Gateway      Metric stat Timer  Use
Route table in VPS00
172.16.37.0    00 24  swp00      172.16.37.206    1    041b 0    1494
127.0.0.0      00 16  swp00      127.0.0.1        1    041b 0     0
0.0.0.0        00 0   swp00      172.16.37.254    1    801b 0   12411
Original Global Route table

```

The following table describes the labels in this screen.

Table 154 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

Subnet-based VLAN Commands

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

72.1 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 58 on page 237](#) for protocol-based VLAN commands and [Chapter 78 on page 297](#) for VLAN commands.

72.2 Command Summary

The following section lists the commands for this feature.

Table 155 subnet-based-vlan Command Summary

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

Table 155 subnet-based-vlan Command Summary (continued)

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

72.3 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

```

Syslog Commands

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

73.1 Command Summary

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

Table 156 syslog User-input Values

COMMAND	DESCRIPTION
<i>type</i>	Possible values: system, interface, switch, aaa, ip.

The following section lists the commands for this feature.

Table 157 syslog Command Summary

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

Table 158 syslog server Command Summary

COMMAND	DESCRIPTION	M	P
syslog server <ip-address> level <level>	Sets the IP address of the syslog server and the severity level. <i>level</i> : 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 159 syslog type Command Summary

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

PART V

Reference T-Z

TACACS+ Commands (285)
TFTP Commands (287)
Trunk Commands (289)
trTCM Commands (293)
VLAN Commands (297)
VLAN IP Commands (303)
VLAN Mapping Commands (305)
VLAN Port Isolation Commands (307)
VLAN Stacking Commands (309)
VLAN Trunking Commands (313)
VRRP Commands (315)
Additional Commands (319)

TACACS+ Commands

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

74.1 Command Summary

The following section lists the commands for this feature.

Table 160 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>]	Specifies the IP address of the specified TACACS+ server. Optionally, sets the port number and key of the TACACS+ server. <i>index</i> : 1 or 2. <i>key-string</i> : 1-32 alphanumeric characters	C	14
tacacs-server mode <index- priority round-robin>	Specifies the mode for TACACS+ server selection.	C	14
tacacs-server timeout <1-1000>	Specifies the TACACS+ server timeout value.	C	14
no tacacs-server <index>	Disables TACACS+ authentication on the specified server.	C	14

Table 161 tacacs-accounting Command Summary

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

TFTP Commands

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

75.1 Command Summary

The following section lists the commands for this feature.

Table 162 tftp Command Summary

COMMAND	DESCRIPTION	M	P
<code>copy tftp flash <ip> <remote-file> [<local-file>]</code>	Restores firmware via TFTP.	E	13
<code>copy tftp config <index> <ip> <remote-file></code>	Restores configuration with the specified filename from the specified TFTP server to the specified configuration file on the Switch. <i>index</i> : 1 or 2 Use <code>reload config <1 2></code> 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
<code>copy tftp config merge <index> <ip> <remote-file></code>	Merges configuration with the specified filename from the specified TFTP server with the specified configuration file on the Switch. <i>index</i> : 1 or 2 Use <code>reload config <1 2></code> 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
<code>copy running-config tftp <ip> <remote-file></code>	Backs up running configuration to the specified TFTP server with the specified file name.	E	13

Trunk Commands

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



Different models support different numbers of trunks (T1, T2, ...). This chapter uses a model that supports six trunks (from T1 to T6).

76.1 Command Summary

The following section lists the commands for this feature.

Table 163 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
trunk <T1 T2 T3 T4 T5 T6> criteria <src-mac dst-mac src-dst-mac src-ip dst-ip src-dst-ip>	Sets the traffic distribution type used for the specified trunk group.	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
trunk <T1 T2 T3 T4 T5 T6> interface <port-list>	Adds a port(s) 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 port(s). <i>lacp-timeout: 1 or 30</i>	C	13

Table 164 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

76.2 Command Examples

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

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

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

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

This example looks at the current trunks.

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

The following table describes the labels in this screen.

Table 165 show trunk

LABEL	DESCRIPTION
Group ID	This field displays the trunk ID number and the current status. inactive: This trunk is disabled. active: This trunk is enabled.
Status	This field displays how the ports were added to the trunk. -: The trunk is disabled. Static: The ports are static members of the trunk. LACP: The ports joined the trunk via LACP.

Table 165 show trunk (continued)

LABEL	DESCRIPTION
Member Number	This field shows the number of ports in the trunk.
Member	This field is displayed if there are ports in the trunk. This field displays the member port(s) in the trunk.

This example shows the current LACP settings.

```

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

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

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

```

The following table describes the labels in this screen.

Table 166 show lacp

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

trTCM Commands

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

77.1 trTCM Overview

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

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

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

77.2 Command Summary

The following section lists the commands for this feature.

Table 167 trtcm Command Summary

COMMAND	DESCRIPTION	M	P
trtcm	Enables trTCM on the Switch.	C	13
trtcm mode <color-aware color-blind>	Sets the mode for trTCM on the Switch.	C	13
no trtcm	Disables trTCM feature on the Switch.	C	13
no trtcm dscp profile <name>	Removes the specified DSCP profile.	C	13
trtcm dscp profile <name> dscp green <0-63> yellow <0-63> red <0-63>	Configures a DSCP profile to specify the DSCP values that you want to assign to packets based on the color they are marked via trTCM	C	13
show interfaces config <port-list> trtcm dscp profile	Displays DSCP profile settings on the specified port(s).	E	3
show trtcm dscp profile	Displays all DSCP profiles settings on the Switch.	E	3
interface port-channel <port-list>	Enters subcommand mode for configuring the specified ports.	C	13
trtcm	Enables trTCM on the specified port(s).	C	13

Table 167 trtcm Command Summary (continued)

COMMAND	DESCRIPTION	M	P
no trtcm	Disables trTCM on the port(s).	C	13
trtcm cir <rate>	Sets the Commit Information Rate on the port(s).	C	13
trtcm pir <rate>	Sets the Peak Information Rate on the port(s).	C	13
trtcm dscp green <0-63>	Specifies the DSCP value to use for packets with low packet loss priority.	C	13
trtcm dscp yellow <0-63>	Specifies the DSCP value to use for packets with medium packet loss priority.	C	13
trtcm dscp red <0-63>	Specifies the DSCP value to use for packets with high packet loss priority.	C	13
trtcm dscp profile <name>	Specifies the DSCP profile that you want to apply to packets on the port(s).	C	13
no trtcm dscp profile	Sets the Switch to apply the default DSCP profile to packets on the port(s).	C	13

77.3 Command Examples

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

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

```

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

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

```

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

- Enable trTCM on the Switch
- Enable Diffserv on the Switch
- Set the Switch to inspect the DSCP value of packets (color-aware mode)
- Create a trTCM DSCP profile with the name “abc”, and set DSCP value 1 for green packets, 2 for yellow packets, 3 for red packets
- Associate the profile “abc” with port 1
- Enable trTCM on port 1
- Enable Diffserv on port 1
- Set the Committed Information Rate (CIR) to 4000 Kpbs
- Set the Peak Information Rate (PIR) to 4500 Kbps
- Display the settings of this example

```

sysname# config
sysname(config)# trtcm
sysname(config)# diffserv
sysname(config)# trtcm mode color-aware
sysname(config)# trtcm dscp profile abc dscp green 1 yellow 2 red 3
sysname(config)# interface port-channel 1
sysname(config-interface)# trtcm
sysname(config-interface)# diffserv
sysname(config-interface)# trtcm dscp profile abc
sysname(config-interface)# trtcm cir 4000
sysname(config-interface)# trtcm pir 4500
sysname(config-interface)# exit
sysname(config)# exit
sysname # show running-config
Building configuration...

Current configuration:

vlan 1
 name 1
 normal ""
 fixed 1-28
 forbidden ""
 untagged 1-28
 ip address default-management 192.168.1.1 255.255.255.0
exit
trtcm
trtcm mode color-aware
trtcm dscp profile abc dscp green 1 yellow 2 red 3
interface port-channel 1
 diffserv
  trtcm
   trtcm cir 4000
   trtcm pir 4500
   trtcm dscp profile abc
exit
diffserv
sysname #

```


VLAN Commands

Use these commands to configure IEEE 802.1Q VLAN.



See [Chapter 79 on page 303](#) for VLAN IP commands.

78.1 VLAN Overview

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



VLAN is unidirectional; it only governs outgoing traffic.

78.2 VLAN Configuration Overview

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

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



See [Chapter 29 on page 125](#) for interface port-channel commands.

78.3 Command Summary

The following section lists the commands for this feature.

Table 168 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 port(s) to be a permanent member of this VLAN group.	C	13
no fixed <port-list>	Sets fixed port(s) to normal port(s).	C	13
forbidden <port-list>	Specifies the port(s) you want to prohibit from joining this VLAN group.	C	13
no forbidden <port-list>	Sets forbidden port(s) to normal port(s).	C	13
inactive	Disables the specified VLAN.	C	13
no inactive	Enables the specified VLAN.	C	13
name <name>	Specifies a name for identification purposes. <i>name</i> : 1-64 English keyboard characters	C	13
normal <port-list>	Specifies the port(s) to dynamically join this VLAN group using GVRP	C	13
untagged <port-list>	Specifies the port(s) you don't want to tag all outgoing frames transmitted with this VLAN Group ID.	C	13
no untagged <port-list>	Specifies the port(s) you want to tag all outgoing frames transmitted with this VLAN Group ID.	C	13
no vlan <vlan-id>	Deletes a VLAN.	C	13

The following section lists the commands for the ingress checking feature



VLAN ingress checking implementation differs across Switch models.

- Some models enable or disable VLAN ingress checking on all the ports via the `vlan1q ingress-check` command.
- Other models enable or disable VLAN ingress checking on each port individually via the `ingress-check` command in the config-interface mode.

Table 169 vlan1q ingress-check Command Summary

COMMAND	DESCRIPTION	M	P
<code>show vlan1q ingress-check</code>	Displays ingress check settings on the Switch.	E	3
<code>vlan1q ingress-check</code>	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
<code>no vlan1q ingress-check</code>	Disables ingress checking on the Switch.	C	13

Table 170 ingress-check Command Summary

COMMAND	DESCRIPTION	M	P
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s).	C	13
<code>ingress-check</code>	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
<code>no ingress-check</code>	Disables ingress checking on the specified ports.	C	13

78.4 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 171 show vlan

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

This example enables ingress checking on ports 1-5.

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

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 172 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	

Table 172 show vlan counters (continued)

LABEL	DESCRIPTION
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.

VLAN IP Commands

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

79.1 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.

79.2 Command Summary

The following section lists the commands for this feature.

Table 173 vlan ip address Command Summary

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

Table 173 vlan ip address Command Summary (continued)

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

79.3 Command Examples

See [Section 3.4 on page 24](#) for an example of how to configure a VLAN management IP address using IPv4. See [Chapter 33 on page 146](#) for IPv6 VLAN commands.

VLAN Mapping Commands

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.



You can not enable VLAN mapping and VLAN stacking at the same time.

80.1 Command Summary

The following section lists the commands for this feature.

Table 174 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
interface port-channel <port-list>	Enters config-interface mode for the specified port(s).	C	13
vlan-mapping	Enables VLAN mapping on the port(s).	C	13
no vlan-mapping	Disables VLAN mapping on the port(s).	C	13

80.2 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)#
```

VLAN Port Isolation Commands

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

81.1 Command Summary

The following section lists the commands for this feature.

Table 175 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 port(s).	C	13
no vlan1q port-isolation	Enables VLAN port isolation on the port(s).	C	13
vlan1q port-isolation	Disables VLAN port isolation on the port(s).	C	13

VLAN Stacking Commands

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

82.1 Command Summary

The following section lists the commands for this feature.

Table 176 vlan-stacking Command Summary

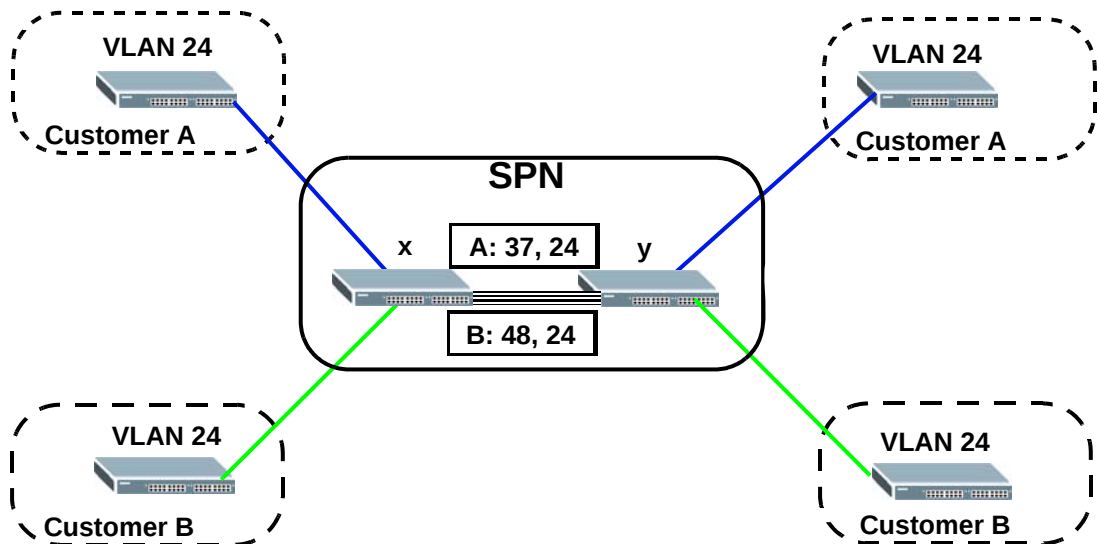
COMMAND	DESCRIPTION	M	P
<code>interface port-channel <port-list></code>	Enters config-interface mode for the specified port(s).	C	13
<code> vlan-stacking priority <0-7></code>	Sets the priority of the specified port(s) in port-based VLAN stacking.	C	13
<code> vlan-stacking role <normal access tunnel></code>	Sets the VLAN stacking port roles of the specified port(s). normal: The Switch ignores frames received (or transmitted) on this port with VLAN stacking tags. access: the Switch adds the SP TPID tag to all incoming frames received on this port. tunnel: (available for Gigabit and faster ports only) for egress ports at the edge of the service provider's network. Note: In order to support VLAN stacking on a port, the port must be able to allow frames of 1526 Bytes (1522 Bytes + 4 Bytes for the second tag) to pass through it.	C	13
<code> vlan-stacking SPVID <1-4094></code>	Sets the service provider VID of the specified port(s).	C	13
<code> vlan-stacking tunnel-tpid <tpid></code>	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 port(s).	C	13
<code>no vlan-stacking</code>	Disables VLAN stacking on the Switch.	C	13
<code>no vlan-stacking selective-qinq interface port-channel <port> cvid <vlan-id></code>	Removes the specified selective VLAN stacking rule.	C	13
<code>no vlan-stacking selective-qinq interface port-channel <port> cvid <vlan-id> inactive</code>	Enables the specified selective VLAN stacking rule.	C	13
<code>show vlan-stacking</code>	Displays VLAN stacking settings.	E	3
<code>vlan-stacking</code>	Enables VLAN stacking on the Switch.	C	13

Table 176 vlan-stacking Command Summary (continued)

COMMAND	DESCRIPTION	M	P
<code>vlan-stacking <sptpid></code>	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
<code>vlan-stacking selective-qinq name <name> interface port-channel <port> cvid <cvid> spvid <spvid> priority <0-7></code>	Creates a selective VLAN stacking rule. <i>cvid</i> : 1 - 4094. This is the VLAN tag carried in the packets from the subscribers. <i>spvid</i> : 1 - 4094: This is the service provider's VLAN ID (the outer VLAN tag).	C	13
<code>vlan-stacking selective-qinq name <name> interface port-channel <port> cvid <cvid> spvid <spvid> priority <0-7> inactive</code>	Disables the specified selective VLAN stacking rule.	C	13

82.2 Command Examples

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag **37** to distinguish customer **A** and tag **48** to distinguish customer **B** at edge device **x** and then stripping those tags at edge device **y** as the data frames leave the network.

Figure 10 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
....			

VLAN Trunking Commands

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

83.1 Command Summary

The following section lists the commands for this feature.

Table 177 vlan-trunking Command Summary

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

VRRP Commands

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

84.1 VRRP Overview

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

84.2 Command Summary

The following section lists the commands for this feature.

Table 178 VRRP Command Summary

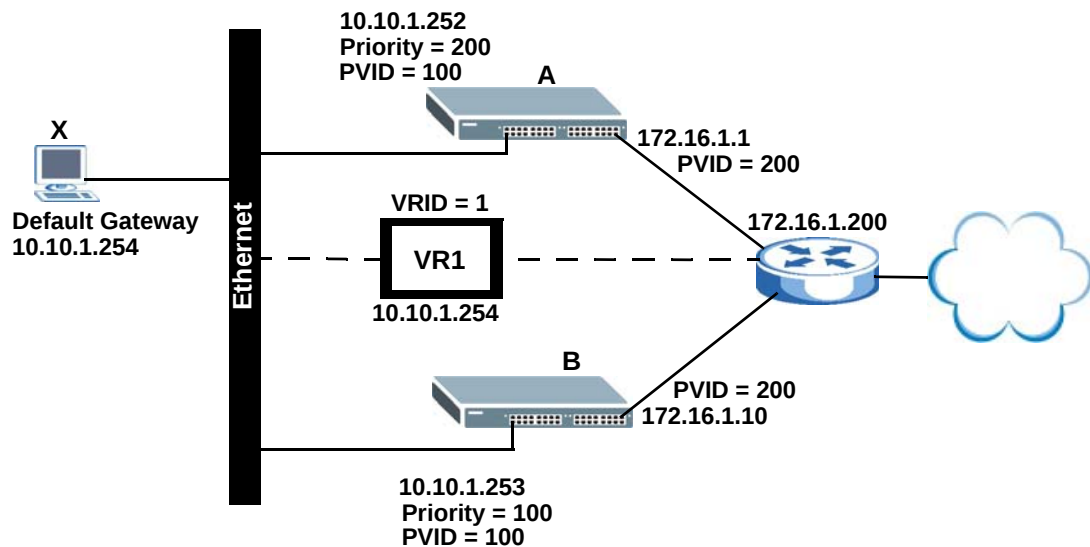
COMMAND	DESCRIPTION	M	P
router vrrp network <ip-address>/<mask-bits> vr-id <1~7> uplink-gateway <ip-address>	Adds a new VRRP network and enters the VRRP configuration mode.	C	13
name <name>	Sets a descriptive name of the VRRP setting for identification purposes.	C	13
priority <1~254>	Sets the priority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

Table 178 VRRP Command Summary (continued)

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

84.3 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 11 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 11 on page 316](#).

```
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 11 on page 316](#).

```
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)#
```

Additional Commands

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

85.1 Command Summary

The following section lists the commands for this feature.

Table 179 Command Summary: Changing Modes or Privileges

COMMAND	DESCRIPTION	M	P
enable	Changes the session's privilege level to 14 and puts the session in enable mode (if necessary). The user has to provide the enable password. See Section 2.1.3.1 on page 18 .	E	0
enable <0-14>	Raises the session's privilege level to the specified level and puts the session in enable mode if the specified level is 13 or 14. The user has to provide the password for the specified privilege level. See Section 2.1.3.2 on page 18 .	E	0
disable	Changes the session's priority level to 0 and changes the mode to user mode. See Section 2.1.3.3 on page 19 .	E	13
configure	Changes the mode to config mode.	E	13
interface port-channel <port-list>	Enters config-interface mode for the specified port(s).	C	13
mvr <1-4094>	Enters config-mvr mode for the specified MVR (multicast VLAN registration). Creates the MVR, if necessary.	C	13
vlan <1-4094>	Enters config-vlan mode for the specified VLAN. Creates the VLAN, if necessary.	C	13
exit	Returns to the previous mode.	C	13
logout	Logs out of the CLI.	E	0

Table 180 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 180 Command Summary: Additional Enable Mode (continued)

COMMAND	DESCRIPTION	M	P
<code>boot image <1 2></code>	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
<code>cable-diagnostics <port-list></code>	Perform a physical wire-pair test of the Ethernet connections on the specified port(s). Ok: The physical connection between the wire-pair is okay. Open: There is no physical connection between the wire-pair.	E	13
<code>ping <ip host-name> [vlan <vlan-id>] [size <0-1472>] [-t]</code>	Sends Ping packets to the specified Ethernet device. <i>vlan-id</i> : Specifies the VLAN ID to which the Ethernet device belongs. <i>size <0-1472></i> : Specifies the size of the Ping packet. <i>-t</i> : Sends Ping packets to the Ethernet device indefinitely. Press [CTRL]+C to terminate the Ping process.	E	0
<code>ping help</code>	Provides more information about the specified command.	E	0
<code>reload config [1 2]</code>	Restarts the system (warm reboot) with the specified configuration file. 1: config-1 2: config-2	E	13
<code>reset slot <slot-list></code>	Restarts the card in the selected slot. The card restarts using the last-saved configuration. Any unsaved changes are lost.	E	13
<code>show allarm-status</code>	Displays alarm status.	E	0
<code>show cpu-utilization</code>	Displays the CPU utilization statistics on the Switch.	E	0
<code>show hardware-monitor <C F></code>	This command is not available in all models. Displays current hardware monitor information with the specified temperature unit (Celsius C or Fahrenheit F).	E	0
<code>show memory</code>	Displays the memory utilization statistics on the Switch.	E	3
<code>show power-source-status</code>	Displays the status of each power module in the system.	E	0
<code>show sfp <port-list></code>	Displays real-time SFP (Small Form Factor Pluggable) transceiver operating parameters on specified SFP port(s). The parameters include, for example, module temperature, module voltage, transmitting and receiving power.	E	3
<code>show interfaces transceiver <port-list></code>	Displays real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on specified SFP port(s). The parameters include, for example, module temperature, module voltage, transmitting and receiving power.	E	3
<code>show slot</code>	Displays general status information about each slot.	E	13
<code>show slot config</code>	Displays what type of card is installed in each slot and its current operational status.	E	13
<code>show slot config <slot-list></code>	Displays detailed information about the specified slots.	E	13
<code>show system-information</code>	Displays general system information.	E	0
<code>show version [flash]</code>	Display the version of the currently running firmware on the Switch. Optionally, display the version of the currently installed firmware on the flash memory.	E	0
<code>test interface port-channel <port-list></code>	Performs an internal loopback test on the specified ports. The test returns Passed! or Failed!.	E	13

Table 180 Command Summary: Additional Enable Mode (continued)

COMMAND	DESCRIPTION	M	P
traceroute <ip host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>]	Determines the path a packet takes to the specified Ethernet device. vlan <vlan-id>: Specifies the VLAN ID to which the Ethernet device belongs. ttl <1-255>: Specifies the Time To Live (TTL) period. wait <1-60>: Specifies the time period to wait. queries <1-10>: Specifies how many times the Switch performs the traceroute function.	E	0
traceroute help	Provides more information about the specified command.	E	0
write memory [<index>]	Saves current configuration in volatile memory to the configuration file the Switch is currently using or the specified configuration file.	E	13

Table 181 Command Summary: Additional Configure Mode

COMMAND	DESCRIPTION	M	P
bcp-transparency	Enables Bridge Control Protocol (BCP) transparency on the Switch.	C	13
default-management <in-band out-of-band>	Sets which traffic flow (in-band or out-of-band) the Switch sends packets originating from itself (such as SNMP traps) or packets with unknown source.	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
no install slot <slot>	Uninstalls the card in the slot.	C	13
mode zynos	Changes the CLI mode to the ZyNOS format.	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
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 via the installed transceiver(s).	C	13

85.2 Command Examples

This example checks the cable pairs on port 7.

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

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

```

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

```

The following table describes the labels in this screen.

Table 182 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 183 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.

Table 183 show alarm-status (continued)

LABEL	DESCRIPTION
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 184 show cpu-utilization

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

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

```

sysname# show hardware-monitor C

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

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

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

```

The following table describes the labels in this screen.

Table 185 show hardware-monitor

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

Table 185 show hardware-monitor (continued)

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

This example displays multicast VLAN configuration on the Switch.

```
sysname> show multicast vlan
Multicast Vlan Status

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

The following table describes the labels in this screen.

Table 186 show multicast vlan

LABEL	DESCRIPTION
Index	This field displays an entry number for the multicast VLAN.
VID	This field displays the multicast VLAN ID.
Type	This field displays what type of multicast VLAN this is. MVR: This VLAN is a Multicast VLAN Registration (MVR). Static: This VLAN is configured via IGMP snooping VLAN in fixed mode. Dynamic: This VLAN is learned dynamically in auto mode. See Chapter 27 on page 115 for more information about IGMP snooping VLAN and IGMP modes.

This example shows the current status of Power over Ethernet.

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

The following table describes the labels in this screen.

Table 187 show poe-status

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

Table 187 show poe-status (continued)

LABEL	DESCRIPTION
Allocated Power	This field displays the total amount of power the Switch has reserved for PoE after negotiating with the PoE device(s). 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.

This example looks at general system information about the Switch

```

sysname# show system-information

Product Model       : XGS-4728F
System Name         : XGS-4728F
System Contact      :
System Location     :
System up Time      :      0:06:21 (9511 ticks)
Ethernet Address    : 00:19:cb:6f:91:59
Bootbase Version    : V1.00 | 10/22/2007
ZyNOS F/W Version   : V4.00(BBC.0)b1 | 10/14/2010
RomRasSize          : 4069634

```

The following table describes the labels in this screen.

Table 188 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 Contact	This field displays the name of the person in charge of this Switch. Use the snmp-server command to configure this. See Chapter 67 on page 263 .
System Location	This field displays the geographic location of this Switch. Use the snmp-server command to configure this. See Chapter 67 on page 263 .
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.
ZyNOS F/W Version	This field displays the firmware version the Switch is running.
RomRasSize	This field displays how much ROM is used.
ZyNOS CODE	This field displays the ZyNOS operating system version the Switch is using.

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: V3.80(BBA.3)b1 | 04/17/2008
```

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

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

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

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

PART VI

Appendices and Index of Commands

[Default Values \(331\)](#)

[Legal Information \(333\)](#)

[Index of Commands \(337\)](#)

Default Values

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

Table 189 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

Legal Information

Copyright

Copyright © 2011 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

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

Trademarks

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

Certifications

Federal Communications Commission (FCC) Interference Statement

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

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

FCC Warning

This device has been tested and found to comply with the limits for a Class A digital switch, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a commercial environment. This device generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this device in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

CE Mark Warning:

This is a class A product. In a domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

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

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

Notices

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

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

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

CLASS 1 LASER PRODUCT

APPAREIL A LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Viewing Certifications

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

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to

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

Note

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

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com.

Index of Commands



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

0	140
001	140
10 bits	140
1111 1110 10	140
16 bits	140
3 bits	140
45 bits	140
54 bits	140
64 bits	140
64 bits	140
8021p-priority <0-7>	201
aaa accounting commands <privilege> stop-only tacacs+ [broadcast]	29
aaa accounting dot1x <start-stop stop-only> <radius tacacs+> [broadcast]	30
aaa accounting exec <start-stop stop-only> <radius tacacs+> [broadcast]	30
aaa accounting system <radius tacacs+> [broadcast]	30
aaa accounting update periodic <1-2147483647>	29
aaa authentication enable <method1> [<method2> ...]	29
aaa authentication login <method1> [<method2> ...]	29
aaa authorization dot1x radius	30
aaa authorization exec <radius tacacs+>	30
admin-password <pw-string>	211
admin-password <pw-string> <confirm-string>	211
admin-password cipher <pw-string>	211
alarm-index	249
area <area-id>	206
area <area-id> authentication	206
area <area-id> authentication message-digest	206
area <area-id> default-cost <0-16777214>	206
area <area-id> name <name>	206
area <area-id> stub	206
area <area-id> stub no-summary	206
area <area-id> virtual-link <router-id> authentication-key <key>	206
area <area-id> virtual-link <router-id>	206
area <area-id> virtual-link <router-ID> authentication-same-as-area	207
area <area-id> virtual-link <router-id> message-digest-key <keyid> md5 <key>	207
area <area-id> virtual-link <router-id> name <name>	207
arp aging-time <60-1000000>	31
arp inspection	33
arp inspection filter-aging-time <1-2147483647>	33
arp inspection filter-aging-time none	33
arp inspection log-buffer entries <0-1024>	34
arp inspection log-buffer logs <0-1024> interval <0-86400>	34
arp inspection trust	34
arp inspection vlan <vlan-list>	34
arp inspection vlan <vlan-list> logging [all none permit deny]	34

arp-learning <arp-reply gratuitous-arp arp-request>	39
bandwidth-control	42
bandwidth-limit cir	42
bandwidth-limit cir <rate>	42
bandwidth-limit egress	42
bandwidth-limit egress <rate>	42
bandwidth-limit ingress	42
bandwidth-limit ingress <rate>	42
bandwidth-limit pir	42
bandwidth-limit pir <rate>	42
baudrate <1 2 3 4 5>	319
bcp-transparency	321
bmstorm-limit	45
bmstorm-limit <rate>	46
boot config <index>	319
boot image <1 2>	320
bpdu-control <peer tunnel discard network>	125
broadcast-limit	46
broadcast-limit <pkt/s>	46
cable-diagnostics <port-list>	320
cc-interval <100ms 1s 10s 1min 10min>	53
classifier <name> <[packet- format <802.3untag 802.3tag EtherIIuntag EtherIItag>] [pri- ority <0-7>] [vlan <vlan-id>] [ethernet-type <ether-num ip ipx arp rarp apple- talk decnet ipv6>] [source-mac <src-mac-addr>] [source-port <port-num>] [destination-mac <dest-mac-addr>] [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]] [source-ip <src-ip-addr> [mask-bits <mask-bits>]] [ipv6-source-ip <src-ipv6-addr> [prefix- length <prefix-length>]] [source-socket <socket-num>] [destination-ip <dest-ip- addr> [mask-bits <mask-bits>]] [ipv6-destination-ip <dest-ipv6-addr> [prefix- length <prefix-length>]] [destination-socket <socket-num>] [inactive]>	59
clear arp inspection filter	33
clear arp inspection log	34
clear arp inspection statistics	33
clear arp inspection statistics vlan <vlan-list>	33
clear cpu-protection interface port-channel <port-list> cause <ARP BPDU IGMP>	86
clear dhcp snooping database statistics	76
clear ethernet cfm linktrace	52
clear ethernet cfm mep-ccmdb	52
clear ethernet cfm mep-defects	52
clear ethernet cfm mip-ccmdb	52
clear igmp-snooping statistics all	115
clear igmp-snooping statistics port	115
clear igmp-snooping statistics system	115
clear igmp-snooping statistics vlan	115
clear interface <port-num>	125
clear ip arp	31
clear ip arp interface port-channel <port-list>	31
clear ip arp ip <ip-address>	31
clear ipv6 mld snooping-proxy statistics all	149
clear ipv6 mld snooping-proxy statistics port	149
clear ipv6 mld snooping-proxy statistics system	149
clear ipv6 mld snooping-proxy statistics vlan	149
clear ipv6 neighbor	154
clear ipv6 neighbor <interface-type> <interface-number>	154
clear l2protocol-tunnel	163
clear lldp remote_info	170
clear lldp remote_info interface port-channel <port-list>	170
clear lldp statistic	170

clear logging	173
clear loopguard	177
clear pppoe intermediate-agent statistics	228
clear pppoe intermediate-agent statistics vlan <vlan-list>	228
cluster <vlan-id>	63
cluster member <mac> password <password>	63
cluster name <cluster name>	63
cluster rcommand <mac>	63
configure	319
copy running-config help	256
copy running-config interface port-channel <port> <port-list> [<attribute> [<...>]]	256
copy running-config slot <slot> <slot-list>	256
copy running-config slot <slot> <slot-list> [bandwidth-limit ...]	256
copy running-config tftp <ip> <remote-file>	287
copy tftp config <index> <ip> <remote-file>	287
copy tftp config merge <index> <ip> <remote-file>	287
copy tftp flash <ip> <remote-file> [<local-file>]	287
cpu-protection cause <ARP BPDU IGMP> rate-limit <0-256>	86
cx4-length <0.5 1 3 5 10 15>	125
default-management <in-band out-of-band>	321
dhcp dhcp-vlan <vlan-id>	76
dhcp relay <vlan-id> helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>] [option] [information]	72
dhcp relay-broadcast	72
dhcp server <vlan-id> starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253>	72
dhcp server <vlan-id> starting-address <ip-addr> <subnet-mask> size-of-client-ip-pool <1-253> [default-gateway <ip-addr>] [primary-dns <ip-addr>] [secondary-dns <ip-addr>]	72
dhcp smart-relay	71
dhcp smart-relay helper-address <remote-dhcp-server1> [<remote-dhcp-server2>] [<remote-dhcp-server3>]	71
dhcp smart-relay information	71
dhcp smart-relay option	71
dhcp snooping	75
dhcp snooping database <tftp://host/filename>	75
dhcp snooping database timeout <seconds>	75
dhcp snooping database write-delay <seconds>	75
dhcp snooping limit rate <pps>	76
dhcp snooping trust	76
dhcp snooping vlan <vlan-list>	76
dhcp snooping vlan <vlan-list> information	76
dhcp snooping vlan <vlan-list> option	76
diffserv	79
diffserv dscp <0-63> priority <0-7>	79
disable	319
display aaa <[authentication][authorization][server]>	81
display user <[system][snmp]>	81
distance <10-255>	207
distance <10-255>	248
dlf-limit	46
dlf-limit <pkt/s>	46
egress set <port-list>	225
enable	319
enable <0-14>	319
erase running-config	256
erase running-config help	256

erase running-config interface port-channel <port-list> [<attribute> [<...>]]	256
errdisable detect cause <ARP BPDU IGMP>	86
errdisable detect cause <ARP BPDU IGMP> mode <inactive-port inactive-reason rate-limitation>	86
errdisable recovery	86
errdisable recovery cause <loopguard ARP BPDU IGMP>	86
errdisable recovery cause <loopguard ARP BPDU IGMP> interval <30-2592000>	86
ethernet cfm	52
ethernet cfm linktrace mac <mac-address> mep <mep-id> ma <ma-index> md <md-index> [mip-ccmdb][[ttl <ttl>]]	52
ethernet cfm linktrace remote-mep <mep-id> mep <mep-id> ma <ma-index> md <md-index> [mip-ccmdb][[ttl <ttl>]]	52
ethernet cfm loopback mac <mac-address> mep <mep-id> ma <ma-index> md <md-index> [size <0-1500>][count <1-1024>]	52
ethernet cfm loopback remote-mep <mep-id> mep <mep-id> ma <ma-index> md <md-index> [size <0-1500>][count <1-1024>]	52
ethernet cfm ma <ma-index> format <vid string integer> name <ma-name> md <md-index> primary-vlan <1-4094>	53
ethernet cfm management-address-domain ip [<ip-addr>]	54
ethernet cfm md <md-index> format <dns mac string> name <md-name> level <0-7>	54
ethernet cfm virtual-mac <mac-addr>	54
ethernet oam	89
ethernet oam	90
ethernet oam mode <active passive>	90
ethernet oam remote-loopback ignore-rx	90
ethernet oam remote-loopback start <port>	89
ethernet oam remote-loopback stop <port>	89
ethernet oam remote-loopback supported	90
ethernet oam remote-loopback test <port> [<number-of-packets> [<packet-size>]]	90
etherstats-index	249
event-index	249
exit	111
exit	131
exit	207
exit	248
exit	316
exit	319
exit	53
external-alarm <index> name <name_string>	95
fe-spq <q0 q1> ... q7>	242
fixed <port-list>	298
flow-control	125
forbidden <port-list>	298
frame-type <all tagged untagged>	125
garp join <100-65535> leave <200-65535> leaveall <200-65535>	97
ge-spq <q0 q1> ... q7>	241
Global ID	140
group <name> start-address <ip> end-address <ip>	201
gvrp	99
help	14
history	14
historycontrol-index	249
hostname <name>	321
https cert-regeneration <rsa dsa>	103
hybrid-spq <q0 q1> ... q7>	241
hybrid-spq lowest-queue <q0 q1> ... q7>	241
id-permission < none chassis management chassis-management>	53
igmp-filtering	123
igmp-filtering profile <name>	123

igmp-filtering profile <name> start-address <ip> end-address <ip>	123
igmp-flush	115
igmp-group-limited	119
igmp-group-limited number <number>	119
igmp-immediate-leave	119
igmp-querier-mode <auto fixed edge>	119
igmp-snooping	115
igmp-snooping 8021p-priority <0-7>	115
igmp-snooping filtering	115
igmp-snooping filtering profile <name> start-address <ip> end-address <ip>	115
igmp-snooping host-timeout <1-16711450>	116
igmp-snooping leave-proxy	116
igmp-snooping leave-timeout <1-16711450>	116
igmp-snooping querier	116
igmp-snooping report-proxy	116
igmp-snooping reserved-multicast-frame <drop flooding>	116
igmp-snooping unknown-multicast-frame <drop flooding>	116
igmp-snooping vlan <vlan-id> [name <name>]	117
igmp-snooping vlan mode <auto fixed>	117
inactive	125
inactive	201
inactive	298
inactive	315
ingress-check	299
install help	321
install slot <slot-list> type <card-type>	321
Interface ID	140
Interface ID	140
interface port-channel <port-list>	112
interface port-channel <port-list>	118
interface port-channel <port-list>	123
interface port-channel <port-list>	125
interface port-channel <port-list>	149
interface port-channel <port-list>	163
interface port-channel <port-list>	168
interface port-channel <port-list>	177
interface port-channel <port-list>	182
interface port-channel <port-list>	187
interface port-channel <port-list>	225
interface port-channel <port-list>	228
interface port-channel <port-list>	237
interface port-channel <port-list>	240
interface port-channel <port-list>	257
interface port-channel <port-list>	293
interface port-channel <port-list>	299
interface port-channel <port-list>	305
interface port-channel <port-list>	307
interface port-channel <port-list>	309
interface port-channel <port-list>	313
interface port-channel <port-list>	319
interface port-channel <port-list>	34
interface port-channel <port-list>	39
interface port-channel <port-list>	42
interface port-channel <port-list>	45
interface port-channel <port-list>	54
interface port-channel <port-list>	76
interface port-channel <port-list>	79
interface port-channel <port-list>	86
interface port-channel <port-list>	90

interface port-channel <port-list>	99
interface route-domain <ip-address>/<mask-bits>	111
interface route-domain <ip-address>/<mask-bits>	131
interface route-domain <ip-address>/<mask-bits>	205
interface route-domain <ip-address>/<mask-bits>	248
interface route-domain <ip-address>/<mask-bits>	83
interface route-domain <ip-address>/<mask-bits> ip vrrp authentication-key <key> ..	316
interface route-domain <ip-address>/<mask-bits> no ip vrrp authentication-key ...	316
interface vlan <1-4094>	146
interface vlan <1-4094>	153
interface-id	249
interval <1-255>	315
intrusion-lock	125
ip address <ip> <mask>	133
ip address <ip-address> <mask>	303
ip address <ip-address> <mask> manageable	303
ip address default-gateway <ip>	133
ip address default-gateway <ip-address>	304
ip address default-management <ip-address> <mask>	303
ip address default-management dhcp-bootp	303
ip address default-management dhcp-bootp release	303
ip address default-management dhcp-bootp renew	303
ip dvmrp	84
ip igmp <v1 v2 v3>	111
ip igmp last-member-query-interval <1-25>	112
ip igmp query-interval	112
ip igmp query-max-response-time <1-25>	112
ip igmp robustness-variable <2-255>	112
ip load-sharing	171
ip load-sharing <sip sip-dip>	171
ip load-sharing aging-time <0-86400>	171
ip load-sharing discover-time <0-86400>	171
ip name-server <ip>	133
ip ospf authentication-key <key>	205
ip ospf authentication-same-aa	205
ip ospf authentication-same-as-area	206
ip ospf cost <1-65535>	206
ip ospf message-digest-key <key>	206
ip ospf priority <0-255>	206
ip policy-route <name>	221
ip policy-route <name> inactive	221
ip policy-route <name> sequence <number> <permit deny> classifier <classifier> next-hop <ip-addr>	221
ip rip direction <Outgoing Incoming Both None> version <v1 v2b v2m>	248
ip route <ip> <mask> <next-hop-ip> [metric <metric>] [name <name>] [inactive] ...	275
ip source binding <mac-addr> vlan <vlan-id> <ip> [interface port-channel <interface-id>] 137	
ip source binding arp-freeze	137
ip source binding arp-freeze interface port-channel <port-list>	137
ip source binding arp-freeze vlan <vlan-list>	137
ipmc egress-untag-vlan <vlan-id>	112
ipv6	146
ipv6 address <ipv6-address>/<prefix>	146
ipv6 address <ipv6-address>/<prefix> eui-64	146
ipv6 address <ipv6-address>/<prefix> link-local	147
ipv6 address autoconfig	147
ipv6 address default-gateway <gateway-ipv6-address>	147
ipv6 address dhcp client <ia-na>	147
ipv6 address dhcp client <ia-na> [rapid-commit]	147

ipv6 address dhcp client information refresh minimum <600-4294967295>	147
ipv6 address dhcp client option <[dns][domain-list]>	147
ipv6 dhcp relay vlan <1-4094> helper-address <remote-dhcp-server>	148
ipv6 dhcp relay vlan <1-4094> option interface-id	148
ipv6 dhcp relay vlan <1-4094> option remote-id <remote-id>	148
ipv6 hop-limit <1-255>	154
ipv6 icmp error-interval <0-2147483647> [bucket-size <1-200>]	149
ipv6 mld snooping-proxy	150
ipv6 mld snooping-proxy 8021p-priority <0-7>	150
ipv6 mld snooping-proxy filtering	150
ipv6 mld snooping-proxy filtering group-limited	149
ipv6 mld snooping-proxy filtering group-limited number <number>	150
ipv6 mld snooping-proxy filtering profile <name>	150
ipv6 mld snooping-proxy filtering profile <name> start-address <ip> end-address <ip> 150	
ipv6 mld snooping-proxy vlan <vlan-id>	150
ipv6 mld snooping-proxy vlan <vlan-id> downstream interface port-channel <port-list> 150	
ipv6 mld snooping-proxy vlan <vlan-id> downstream interface port-channel <port-list> fast-leave-timeout <2-16775168>	150
ipv6 mld snooping-proxy vlan <vlan-id> downstream interface port-channel <port-list> leave-timeout <2-16775168>	150
ipv6 mld snooping-proxy vlan <vlan-id> downstream interface port-channel <port-list> mode <immediate normal fast>	150
ipv6 mld snooping-proxy vlan <vlan-id> downstream query-interval <1000-31744000>	150
ipv6 mld snooping-proxy vlan <vlan-id> downstream query-max-response-time <1000-25000> 150	
ipv6 mld snooping-proxy vlan <vlan-id> upstream interface port-channel <port-list>	151
ipv6 mld snooping-proxy vlan <vlan-id> upstream last-listener-query-interval <1-8387584> 151	
ipv6 mld snooping-proxy vlan <vlan-id> upstream query-interval <1000-31744000> ..	151
ipv6 mld snooping-proxy vlan <vlan-id> upstream query-max-response-time <1000-25000> 151	
ipv6 mld snooping-proxy vlan <vlan-id> upstream robustness-variable <1-25>	151
ipv6 neighbor <interface-type> <interface-number> <ipv6-address> <mac-address> ..	155
ipv6 route <ipv6-prefix>/<prefix-length> <next-hop>	154
ipv6 route <ipv6-prefix>/<prefix-length> <next-hop> <interface-type> <interface-number> 154	
kick tcp <session id>	134
l2protocol-tunnel	163
l2protocol-tunnel	164
l2protocol-tunnel cdp	163
l2protocol-tunnel mac <mac-addr>	164
l2protocol-tunnel mode <access tunnel>	163
l2protocol-tunnel point-to-point	163
l2protocol-tunnel point-to-point lacp	163
l2protocol-tunnel point-to-point pagp	163
l2protocol-tunnel point-to-point udld	164
l2protocol-tunnel stp	164
l2protocol-tunnel vtp	164
lacp	290
lacp system-priority <1-65535>	290
lldp	169
lldp admin-status <tx-only rx-only tx-rx>	168
lldp basic-tlv management-address	168
lldp basic-tlv port-description	168
lldp basic-tlv system-capabilities	168
lldp basic-tlv system-description	168
lldp basic-tlv system-name	168

lldp notification	168
lldp org-specific-tlv dot1 port-protocol-vlan-id	168
lldp org-specific-tlv dot1 port-vlan-id	168
lldp org-specific-tlv dot3 link-aggregation	168
lldp org-specific-tlv dot3 mac-phy	168
lldp org-specific-tlv dot3 max-frame-size	168
lldp org-specific-tlv dot3 power-via-mdi	168
lldp reinitialize-delay <1-10>	169
lldp transmit-delay <1-8192>	169
lldp transmit-hold <2-10>	169
lldp transmit-interval <5-32768>	169
logins username <name> password <password> privilege <0-14>	175
logins username <name> password cipher <password> privilege <0-14>	175
logout	319
loopguard	177
loopguard	177
mac-address	51
mac-aging-time <10-1000000>	179
mac-authentication	181
mac-authentication	182
mac-authentication nameprefix <name-string>	181
mac-authentication password <name-string>	181
mac-authentication timeout <1-3000>	181
mac-filter name <name> mac <mac-addr> vlan <vlan-id>	183
mac-filter name <name> mac <mac-addr> vlan <vlan-id> drop <src dst both>	183
mac-filter name <name> mac <mac-addr> vlan <vlan-id> inactive	183
mac-flush [<port-num>]	179
mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id>	185
mac-forward name <name> mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive	185
mac-transfer dynamic-to-filter interface port-channel <port-list>	179
mac-transfer dynamic-to-filter mac <mac-addr>	179
mac-transfer dynamic-to-filter vlan <vlan-list>	179
mac-transfer dynamic-to-forward interface port-channel <port-list>	180
mac-transfer dynamic-to-forward mac <mac-addr>	179
mac-transfer dynamic-to-forward vlan <vlan-list>	180
ma-index	51
md-index	51
mep <mep-id> interface port-channel <port> direction <up down> priority <0-7>	53
mep <mep-id> interface port-channel <port> direction <up down> priority <0-7> cc-enable	53
mep <mep-id> interface port-channel <port> direction <up down> priority <0-7> inactive	53
mep-id	51
mhf-creation < none default explicit>	53
mirror	187
mirror dir <ingress egress both>	188
mirror-filter egress mac <mac-addr>	188
mirror-filter egress type <all dest src>	188
mirror-filter ingress mac <mac-addr>	188
mirror-filter ingress type <all dest src>	188
mirror-port	187
mirror-port <port-num>	187
mode <dynamic compatible>	201
mode zynos	321
mrstp <tree-index>	191
mrstp <tree-index> hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	191
mrstp <tree-index> priority <0-61440>	191
mrstp interface <port-list>	191

mrstp interface <port-list> edge-port	192
mrstp interface <port-list> path-cost <1-65535>	192
mrstp interface <port-list> priority <0-255>	192
mrstp interface <port-list> tree-index <tree-index>	192
mstp	193
mstp configuration-name <name>	193
mstp hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	193
mstp instance <number> interface port-channel <port-list>	194
mstp instance <number> interface port-channel <port-list> path-cost <1-65535> ...	194
mstp instance <number> interface port-channel <port-list> priority <1-255>	194
mstp instance <number> priority <0-61440>	194
mstp instance <number> vlan <vlan-list>	194
mstp interface port-channel <port-list> edge-port	193
mstp max-hop <1-255>	193
mstp revision <0-65535>	193
multicast-forward name <name> mac <mac-addr> vlan <vlan-id> inactive	273
multicast-forward name <name> mac <mac-addr> vlan <vlan-id> interface port-channel <port-	
list>	273
multicast-limit	46
multicast-limit <pkt/s>	46
multi-login	199
mvr <1-4094>	319
mvr <vlan-id>	201
name <name>	201
name <name>	298
name <name>	315
name <port-name-string>	125
network <ip-addr/bits> area <area-id>	207
no aaa accounting commands	30
no aaa accounting dot1x	30
no aaa accounting exec	30
no aaa accounting system	30
no aaa accounting update	29
no aaa accounting update	331
no aaa authentication enable	29
no aaa authentication enable	331
no aaa authentication login	29
no aaa authentication login	331
no aaa authorization dot1x	30
no aaa authorization exec	30
no area <area-id>	206
no area <area-id> authentication	206
no area <area-id> default-cost	206
no area <area-id> stub	206
no area <area-id> stub no-summary	206
no area <area-id> virtual-link <router-id>	206
no area <area-id> virtual-link <router-id> authentication-key	207
no area <area-id> virtual-link <router-id> authentication-same-as-area	207
no area <area-id> virtual-link <router-id> message-digest-key	207
no arp	31
no arp inspection	33
no arp inspection filter <mac-addr> vlan <vlan-id>	33
no arp inspection filter-aging-time	33
no arp inspection filter-aging-time	331
no arp inspection log-buffer entries	331
no arp inspection log-buffer entries	34
no arp inspection log-buffer logs	331
no arp inspection log-buffer logs	34
no arp inspection trust	34

no arp inspection vlan <vlan-list>	34
no arp inspection vlan <vlan-list> logging	34
no arp-learning	39
no bandwidth-control	42
no bandwidth-limit cir	42
no bandwidth-limit egress	42
no bandwidth-limit ingress	42
no bandwidth-limit pir	42
no bmstorm-limit	46
no broadcast-limit	46
no classifier <name>	59
no classifier <name> inactive	59
no cluster	63
no cluster member <mac>	63
no dhcp dhcp-vlan	76
no dhcp relay <vlan-id>	72
no dhcp relay <vlan-id> information	72
no dhcp relay <vlan-id> option	72
no dhcp relay-broadcast	72
no dhcp server <vlan-id>	72
no dhcp server <vlan-id> default-gateway	72
no dhcp server <vlan-id> primary-dns	72
no dhcp server <vlan-id> secondary-dns	72
no dhcp smart-relay	71
no dhcp smart-relay information	71
no dhcp smart-relay option	71
no dhcp snooping	75
no dhcp snooping database	75
no dhcp snooping database timeout <seconds>	75
no dhcp snooping database write-delay <seconds>	75
no dhcp snooping limit rate	76
no dhcp snooping trust	76
no dhcp snooping vlan <vlan-list>	76
no dhcp snooping vlan <vlan-list> information	76
no dhcp snooping vlan <vlan-list> option	76
no diffserv	79
no diffserv	79
no display aaa <[authentication][authorization][server]>	81
no display user <[system][snmp]>	81
no dlf-limit	46
no egress set <port-list>	225
no errdisable detect cause <ARP BPDU IGMP>	86
no errdisable recovery	86
no errdisable recovery cause <loopguard ARP BPDU IGMP>	86
no ethernet cfm	54
no ethernet cfm ma <ma-index> md <md-index>	54
no ethernet cfm management-address-domain	54
no ethernet cfm md <md-index>	54
no ethernet cfm virtual-mac	54
no ethernet oam	89
no ethernet oam	90
no ethernet oam mode	90
no ethernet oam remote-loopback ignore-rx	90
no ethernet oam remote-loopback supported	90
no external-alarm <index>	95
no external-alarm all	95
no fixed <port-list>	298
no flow-control	126
no forbidden <port-list>	298

no group	201
no group <name-str>	201
no gvrp	99
no hybrid-spq	241
no igmp-filtering	123
no igmp-filtering profile	123
no igmp-filtering profile <name>	123
no igmp-filtering profile <name> start-address <ip> end-address <ip>	123
no igmp-group-limited	119
no igmp-immediate-leave	119
no igmp-snooping	115
no igmp-snooping 8021p-priority	115
no igmp-snooping filtering	115
no igmp-snooping filtering profile <name>	115
no igmp-snooping filtering profile <name> start-address <ip> end-address <ip> ...	115
no igmp-snooping leave-proxy	116
no igmp-snooping querier	116
no igmp-snooping report-proxy	116
no igmp-snooping vlan <vlan-id>	117
no inactive	126
no inactive	201
no inactive	298
no inactive	315
no ingress-check	299
no install slot <slot>	321
no interface <port-num>	126
no intrusion-lock	126
no ip address <ip-address> <mask>	303
no ip address default-gateway	304
no ip address default-management dhcp-bootp	303
no ip dvmrp	84
no ip igmp	112
no ip load-sharing	171
no ip ospf authentication-key <key>	205
no ip ospf authentication-same-aa	206
no ip ospf authentication-same-as-area	206
no ip ospf cost <1-65535>	206
no ip ospf message-digest-key <key>	206
no ip ospf priority <0-255>	206
no ip policy-route <name>	221
no ip policy-route <name> inactive	221
no ip policy-route <name> sequence <number>	221
no ip route <ip> <mask>	275
no ip route <ip> <mask> <next-hop-ip>	275
no ip route <ip> <mask> <next-hop-ip> inactive	275
no ip route <ip> <mask> inactive	275
no ip source binding <mac-addr> vlan <vlan-id>	137
no ipmc egress-untag-vlan	112
no ipv6	147
no ipv6 address <ipv6-address>/<prefix>	147
no ipv6 address <ipv6-address>/<prefix> eui-64	147
no ipv6 address <ipv6-address>/<prefix> link-local	147
no ipv6 address autoconfig	147
no ipv6 address default-gateway	147
no ipv6 address dhcp client	147
no ipv6 address dhcp client [rapid-commit]	147
no ipv6 address dhcp client option	147
no ipv6 address dhcp client option <[dns][domain-list]>	147
no ipv6 dhcp relay vlan <1-4094>	148

no ipv6 dhcp relay vlan <1-4094> option interface-id	148
no ipv6 dhcp relay vlan <1-4094> option remote-id	148
no ipv6 hop-limit	154
no ipv6 mld snooping-proxy	151
no ipv6 mld snooping-proxy filtering	151
no ipv6 mld snooping-proxy filtering group-limited	150
no ipv6 mld snooping-proxy filtering profile	150
no ipv6 mld snooping-proxy filtering profile <name>	152
no ipv6 mld snooping-proxy filtering profile <name> start-address <ip> end-address <ip> 152	
no ipv6 mld snooping-proxy vlan <vlan-id>	152
no ipv6 mld snooping-proxy vlan <vlan-id> downstream interface port-channel <port-list> 152	
no ipv6 mld snooping-proxy vlan <vlan-id> upstream interface port-channel <port-list> 152	
no ipv6 neighbor <interface-type> <interface-number> <ipv6-address>	155
no ipv6 route <ipv6-prefix>/<prefix-length>	154
no l2protocol-tunnel	164
no l2protocol-tunnel	164
no l2protocol-tunnel cdp	164
no l2protocol-tunnel point-to-point	164
no l2protocol-tunnel point-to-point lacp	164
no l2protocol-tunnel point-to-point pagp	164
no l2protocol-tunnel point-to-point udld	164
no l2protocol-tunnel stp	164
no l2protocol-tunnel vtp	164
no lacp	290
no lldp	169
no lldp admin-status	168
no lldp basic-tlv management-address	168
no lldp basic-tlv port-description	168
no lldp basic-tlv system-capabilities	168
no lldp basic-tlv system-description	168
no lldp basic-tlv system-name	169
no lldp notification	169
no lldp org-specific-tlv dot1 port-protocol-vlan-id	169
no lldp org-specific-tlv dot1 port-vlan-id	169
no lldp org-specific-tlv dot3 link-aggregation	169
no lldp org-specific-tlv dot3 mac-phy	169
no lldp org-specific-tlv dot3 max-frame-size	169
no lldp org-specific-tlv dot3 power-via-mdi	169
no logging	173
no logins username <name>	175
no loopguard	177
no loopguard	177
no mac-authentication	181
no mac-authentication	182
no mac-authentication timeout	182
no mac-filter mac <mac-addr> vlan <vlan-id>	183
no mac-filter mac <mac-addr> vlan <vlan-id> inactive	183
no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id>	185
no mac-forward mac <mac-addr> vlan <vlan-id> interface <interface-id> inactive ..	185
no mep <mep-id>	53
no mep <mep-id> cc-enable	53
no mep <mep-id> inactive	53
no mirror	188
no mirror-port	187
no mirror-port <port-num>	187
no mrstp <tree-index>	192

no mrstp interface <port-list>	192
no mrstp interface <port-list> edge-port	192
no mstp	193
no mstp instance <number>	194
no mstp instance <number> interface port-channel <port-list>	194
no mstp instance <number> vlan <1-4094>	194
no mstp interface port-channel <port-list> edge-port	193
no multicast-forward mac <mac-addr> vlan <vlan-id>	273
no multicast-forward mac <mac-addr> vlan <vlan-id> inactive	273
no multicast-limit	46
no multi-login	199
no mvr <vlan-id>	201
no network <ip-addr/bits>	207
no non-querier	111
no passive-iface <ip-addr/bits>	208
no password encryption	211
no password privilege <0-14>	211
no policy <name>	219
no policy <name> inactive	219
no port-access-authenticator	107
no port-access-authenticator <port-list>	107
no port-access-authenticator <port-list> guest-vlan	107
no port-access-authenticator <port-list> guest-vlan Host-mode	107
no port-access-authenticator <port-list> reauthenticate	107
no port-security	223
no port-security <port-list>	223
no port-security <port-list> learn inactive	223
no port-security <port-list> vlan <vlan-id> address-limit	224
no port-security <port-list> vlan <vlan-id> address-limit inactive	224
no pppoe intermediate-agent	228
no pppoe intermediate-agent format-type access-node-identifier	229
no pppoe intermediate-agent format-type circuit-id	228
no pppoe intermediate-agent format-type identifier-string	229
no pppoe intermediate-agent format-type remote-id	228
no pppoe intermediate-agent trust	228
no pppoe intermediate-agent vlan <vlan-id> format-type circuit-id	228
no pppoe intermediate-agent vlan <vlan-id> format-type remote-id	228
no pppoe intermediate-agent vlan <vlan-list>	229
no pppoe intermediate-agent vlan <vlan-list> circuit-id	229
no pppoe intermediate-agent vlan <vlan-list> remote-id	228
no pppoe intermediate-agent vlan <vlan-list> remote-id	229
no preempt	316
no primary-virtual-ip	315
no primary-virtual-ip <ip-address>	315
no private-vlan <vlan-id>	234
no private-vlan <vlan-id> inactive	234
no protocol-based-vlan ethernet-type <ether-num ip ipx arp rarp appletalk decnet>	238
no pwr interface <port-list>	213
no pwr mibtrap	213
no radius-accounting <index>	244
no radius-accounting <index>	331
no radius-server <index>	243
no radius-server <index>	331
no receiver-port <port-list>	201
no redistribute rip	207
no redistribute static	208
no remote-management <index>	245
no remote-management <index> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	

no remote-mep <mep-id>	53
no rmon alarm alarmtable <alarm-index>	250
no rmon event eventtable <event-index>	250
no rmon history historycontrol <historycontrol-index>	250
no rmon statistics etherstats <etherstats-index>	250
no router dvmrp	83
no router igmp	111
no router ospf	208
no router rip	248
no router vrrp network <ip-address>/<mask-bits> vr-id <1-7>	316
no secondary-virtual-ip	315
no service-control ftp	246
no service-control http	246
no service-control https	246
no service-control icmp	246
no service-control snmp	246
no service-control ssh	246
no service-control telnet	246
no sflow	257
no sflow	257
no sflow collector <ip-address>	257
no sflow collector <ip-address>	258
no shutdown slot <slot-list>	321
no smart-isolation	260
no snmp-server trap-destination <ip>	264
no snmp-server trap-destination <ip> enable traps	264
no snmp-server trap-destination <ip> enable traps aaa	264
no snmp-server trap-destination <ip> enable traps aaa <options>	265
no snmp-server trap-destination <ip> enable traps interface	265
no snmp-server trap-destination <ip> enable traps interface <options>	265
no snmp-server trap-destination <ip> enable traps ip	265
no snmp-server trap-destination <ip> enable traps ip <options>	265
no snmp-server trap-destination <ip> enable traps switch	265
no snmp-server trap-destination <ip> enable traps switch <options>	265
no snmp-server trap-destination <ip> enable traps system	265
no snmp-server trap-destination <ip> enable traps system <options>	265
no snmp-server username <name>	264
no source-port <port-list>	201
no spanning-tree	267
no spanning-tree <port-list>	267
no spanning-tree <port-list> edge-port	268
no ssh key <rsa rsa dsa>	271
no ssh known-hosts <host-ip>	271
no ssh known-hosts <host-ip> <1024 ssh-rsa ssh-dsa>	271
no storm-control	45
no subnet-based-vlan	279
no subnet-based-vlan dhcp-vlan-override	280
no subnet-based-vlan source-ip <ip> mask-bits <mask-bits>	280
no syslog	281
no syslog server <ip-address>	281
no syslog server <ip-address> inactive	281
no syslog type <type>	281
no tacacs-accounting <index>	285
no tacacs-server <index>	285
no tagged <port-list>	201
no time daylight-saving-time	68
no timesync	68
no trtcm	293
no trtcm	294

no trtcm dscp profile	294
no trtcm dscp profile <name>	293
no trunk <T1 T2 T3 T4 T5 T6>	289
no trunk <T1 T2 T3 T4 T5 T6> criteria	289
no trunk <T1 T2 T3 T4 T5 T6> interface <port-list>	289
no trunk <T1 T2 T3 T4 T5 T6> lacp	289
no untagged <port-list>	298
no vlan <vlan-id>	298
no vlan1q gvrp	99
no vlan1q ingress-check	299
no vlan1q port-isolation	307
no vlan-mapping	305
no vlan-mapping interface port-channel <port> vlan <1-4094>	305
no vlan-mapping interface port-channel <port> vlan <1-4094> inactive	305
no vlan-stacking	309
no vlan-stacking selective-qinq interface port-channel <port> cvid <vlan-id>	309
no vlan-stacking selective-qinq interface port-channel <port> cvid <vlan-id> inactive	309
no vlan-trunking	313
non-querier	111
normal <port-list>	298
owner	249
passive-iface <ip-addr/bits>	208
password <password> [privilege <0-14>]	211
password cipher <pw-string> [privilege <0-14>]	211
password encryption	211
ping <ip host-name> [vlan <vlan-id>] [size <0-1472>] [-t]	320
ping help	320
ping6 <ipv6-address> <[-i <interface-type> <interface-number>] [-t] [-l <1-1452>] [-n	
<1-65535>] [-s <ipv6-address>]	149
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]>	219
policy <name> classifier <classifier-list> <[vlan <vlan-id>][egress-port <port-	
num>][priority <0-7>][dscp <0-63>][tos <0-7>][bandwidth <bandwidth>][egress-mask	
<port-list>][outgoing-packet-format <tagged untagged>][out-of-profile-dscp <0-	
63>][forward-action <drop forward egressmask>][queue-action <prio-set prio-	
queue prio-replace-tos>][diffserv-action <diff-set-tos diff-replace-priori-	
ty diff-set-dscp>][outgoing-mirror][outgoing-eport][outgoing-non-unicast-ep-	
ort][outgoing-set-vlan][metering][out-of-profile-action <[change-dscp][drop][	
forward] [set-drop-precedence]>][inactive]>	218
port-access-authenticator	107
port-access-authenticator <port-list>	108
port-access-authenticator <port-list> guest-vlan	108
port-access-authenticator <port-list> guest-vlan <vlan-id>	108
port-access-authenticator <port-list> guest-vlan Host-mode Multi-host	108
port-access-authenticator <port-list> guest-vlan Host-mode Multi-secure [<1-24>]	108
port-access-authenticator <port-list> max-req <1-10>	108
port-access-authenticator <port-list> quiet-period <0-65535>	108
port-access-authenticator <port-list> reauthenticate	108
port-access-authenticator <port-list> reauth-period <1-65535>	108
port-access-authenticator <port-list> supp-timeout <30-65535>	108
port-access-authenticator <port-list> tx-period <1-65535>	108
port-security	223
port-security <port-list>	223
port-security <port-list> address-limit <number>	223
port-security <port-list> learn inactive	223
port-security <port-list> MAC-freeze	223
port-security <port-list> vlan <vlan-id> address-limit <number>	223

port-security <port-list> vlan <vlan-id> address-limit <number> inactive	224
pppoe intermediate-agent	229
pppoe intermediate-agent format-type access-node-identifier string <string>	229
pppoe intermediate-agent format-type circuit-id string <string>	228
pppoe intermediate-agent format-type identifier-string string <string> option <sp sv pv spv> delimiter <# . , ; / >	229
pppoe intermediate-agent format-type remote-id string <string>	228
pppoe intermediate-agent trust	228
pppoe intermediate-agent vlan <vlan-id> format-type circuit-id string <string> ..	228
pppoe intermediate-agent vlan <vlan-id> format-type remote-id string <string> ...	228
pppoe intermediate-agent vlan <vlan-list>	229
pppoe intermediate-agent vlan <vlan-list> circuit-id	229
pppoe intermediate-agent vlan <vlan-list> remote-id	229
preempt	316
primary-virtual-ip <ip-address>	315
priority <1-254>	315
private-vlan name <name> vlan <vlan-id>	234
private-vlan name <name> vlan <vlan-id> inactive	234
private-vlan name <name> vlan <vlan-id> promiscuous-port <port-list>	234
private-vlan name <name> vlan <vlan-id> promiscuous-port <port-list> inactive ...	234
protocol-based-vlan name <name> ethernet-type <ether-num ip ipx arp rarp appletalk dec- net> vlan <vlan-id> priority <0-7>	238
pvid <1-4094>	126
pwr interface <port-list>	213
pwr interface <port-list> priority <critical high low>	213
pwr mibtrap	213
pwr mode <classification consumption>	213
pwr usagethreshold <1-99>	213
qos priority <0-7>	126
queue priority <0-7> level <0-7>	240
queue priority <0-7> level <0-7>	242
radius-accounting host <index> <ip> [acct-port <socket-number>] [key <key-string>]	244
radius-accounting timeout <1-1000>	243
radius-server host <index> <ip> [auth-port <socket-number>] [key <key-string>] ..	243
radius-server mode <index-priority round-robin>	243
radius-server timeout <1-1000>	243
receiver-port <port-list>	201
redistribute rip	207
redistribute rip metric-type <1 2> metric <0-16777214>	207
redistribute static	208
redistribute static metric-type <1 2> metric <0-16777214>	208
reload config [1 2]	320
remote-management <index>	245
remote-management <index> start-addr <ip> end-addr <ip> service <[telnet] [ftp] [http] [icmp] [snmp] [ssh] [https]>	245
remote-mep <mep-id>	53
renew dhcp snooping database	76
renew dhcp snooping database <tftp://host/filename>	76
reset cpu-protection interface port-channel <port-list> cause <ARP BPDU IGMP>	86
reset slot <slot-list>	320
restart ipv6 dhcp client vlan <1-4094>	147
rmon alarm alarmtable <alarm-index> variable <variable> interval <interval-integer> sam- ple-type <absolute delta> startup-alarm <startup-alarm> rising-threshold <rising- integer> <event-index> falling-threshold <falling-integer> <event-index> [owner <owner>]	250
rmon alarm alarmtable <alarm-index> variable <variable> interval <interval-integer> sam- ple-type <absolute delta> startup-alarm <startup-alarm> rising-threshold <rising- integer> <event-index> falling-threshold <falling-integer> <event-index> [owner <owner>]	251

rmon event eventtable <event-index> [log] [trap <community>] [owner <owner>] [description <description>]	250
rmon history historycontrol <historycontrol-index> buckets <1-65535> interval <1-3600> port-channel <interface-id> [owner <owner>]	250
rmon statistics etherstats <etherstats-index> port-channel <interface-id> [owner <owner>]	250
router dvmrp	83
router igmp	111
router ospf <router-id>	206
router rip	247
router vrrp network <ip-address>/<mask-bits> vr-id <1-7> uplink-gateway <ip-address>	315
secondary-virtual-ip <ip-address>	315
service-control ftp	245
service-control ftp <socket-number>	245
service-control http	246
service-control http <socket-number> <timeout>	246
service-control https	246
service-control https <socket-number>	246
service-control icmp	246
service-control snmp	246
service-control ssh	246
service-control ssh <socket-number>	246
service-control telnet	246
service-control telnet <socket-number>	246
sflow	257
sflow	258
sflow collector <ip-address> [poll-interval <20-120>] [sample-rate <256-65535>]	257
sflow collector <ip-address> [udp-port <udp-port>]	258
show aaa accounting	29
show aaa accounting commands	29
show aaa accounting dot1x	30
show aaa accounting exec	30
show aaa accounting system	30
show aaa accounting update	29
show aaa authentication	29
show aaa authentication enable	29
show aaa authentication login	29
show aaa authorization	30
show aaa authorization dot1x	30
show aaa authorization exec	30
show allarm-status	320
show arp inspection	33
show arp inspection filter [<mac-addr>] [vlan <vlan-id>]	33
show arp inspection interface port-channel <port-list>	34
show arp inspection log	34
show arp inspection statistics	33
show arp inspection statistics vlan <vlan-list>	33
show arp inspection vlan <vlan-list>	34
show classifier [<name>]	59
show cluster	63
show cluster candidates	63
show cluster member	63
show cluster member config	63
show cluster member mac <mac>	63
show cpu-protection interface port-channel <port-list>	86
show cpu-utilization	320
show dhcp relay <vlan-id>	72
show dhcp server	72

show dhcp server <vlan-id>	72
show dhcp smart-relay	71
show dhcp snooping	75
show dhcp snooping binding	75
show dhcp snooping database	75
show dhcp snooping database detail	75
show diffserv	79
show errdisable	87
show errdisable detect	87
show errdisable recovery	87
show ethernet cfm linktrace	54
show ethernet cfm local	54
show ethernet cfm local stack	54
show ethernet cfm local stack mep	54
show ethernet cfm local stack mep <mep-id> ma <ma-index> md <md-index>	54
show ethernet cfm local stack mep <mep-id> ma <ma-index> md <md-index> mep-ccmdb [remote- mep <mep-id>]	54
show ethernet cfm local stack mip	54
show ethernet cfm local stack mip mip-ccmdb	54
show ethernet cfm remote	54
show ethernet cfm virtual-mac	54
show ethernet cfm virtual-mac port <port-list>	54
show ethernet oam discovery <port-list>	89
show ethernet oam statistics <port-list>	89
show ethernet oam summary	89
show external-alarm	95
show garp	97
show hardware-monitor <C F>	320
show https	103
show https certificate	103
show https key <rsa dsa>	103
show https session	103
show igmp-filtering profile	123
show igmp-snooping	116
show igmp-snooping filtering profile	116
show igmp-snooping group all	116
show igmp-snooping group client < [vlan <vlan-list>] [interface port-channel <port- list>] [multicast-group <group-address>] >	116
show igmp-snooping group client all	116
show igmp-snooping group count	116
show igmp-snooping group interface port-channel <port-list>	117
show igmp-snooping group interface port-channel <port-list> count	117
show igmp-snooping group vlan <vlan-list>	117
show igmp-snooping group vlan <vlan-list> count	117
show igmp-snooping querier	117
show igmp-snooping statistics interface port-channel <port-list>	117
show igmp-snooping statistics system	117
show igmp-snooping statistics vlan <vlan-list>	117
show igmp-snooping vlan	117
show interfaces <port-list>	126
show interfaces config <port-list>	126
show interfaces config <port-list> bandwidth-control	42
show interfaces config <port-list> bstorm-control	45
show interfaces config <port-list> egress	225
show interfaces config <port-list> igmp-filtering	123
show interfaces config <port-list> igmp-group-limited	117
show interfaces config <port-list> igmp-immediate-leave	117
show interfaces config <port-list> igmp-query-mode	118
show interfaces config <port-list> igmp-snooping filtering	118

show interfaces config <port-list> igmp-snooping group-limited	118
show interfaces config <port-list> igmp-snooping leave-mode	118
show interfaces config <port-list> igmp-snooping query-mode	118
show interfaces config <port-list> protocol-based-vlan	237
show interfaces config <port-list> trtcm dscp profile	293
show interfaces transceiver <port-list>	320
show ip	133
show ip arp	31
show ip dvmrp group	83
show ip dvmrp interface	83
show ip dvmrp neighbor	83
show ip dvmrp prune	83
show ip dvmrp route	83
show ip igmp group	112
show ip igmp interface	112
show ip igmp multicast	112
show ip igmp timer	112
show ip iptable all [IP VID PORT]	133
show ip iptable count	133
show ip iptable static	133
show ip ospf database	205
show ip ospf interface	205
show ip ospf neighbor	205
show ip policy-route	221
show ip policy-route <name>	221
show ip policy-route <name> sequence <number>	221
show ip protocols	205
show ip protocols	247
show ip route	275
show ip route static	275
show ip source binding [<mac-addr>] [...]	137
show ip source binding help	137
show ip tcp	133
show ip udp	134
show ipv6	147
show ipv6 <interface-type> <interface-number>	148
show ipv6 dhcp	148
show ipv6 dhcp vlan <1-4094>	148
show ipv6 mld snooping-proxy	152
show ipv6 mld snooping-proxy filtering profile	152
show ipv6 mld snooping-proxy group	152
show ipv6 mld snooping-proxy statistics interface port-channel <port-list>	152
show ipv6 mld snooping-proxy statistics system	152
show ipv6 mld snooping-proxy statistics vlan <vlan-list>	152
show ipv6 mld snooping-proxy vlan <vlan-id>	152
show ipv6 mtu	149
show ipv6 multicast	152
show ipv6 neighbor	155
show ipv6 neighbor <interface-type> <interface-number>	155
show ipv6 prefix	154
show ipv6 prefix <interface-type> <interface-number>	154
show ipv6 route	154
show ipv6 route static	154
show ipv6 router	155
show ipv6 router <interface-type> <interface-number>	155
show l2protocol-tunnel	164
show l2protocol-tunnel interface port-channel <port-list>	164
show lacp	290
show lldp config	169

show lldp config interface port-channel <port-list>	169
show lldp info local	169
show lldp info local interface port-channel <port-list>	169
show lldp info remote	169
show lldp info remote interface port-channel <port-list>	169
show lldp statistic	169
show lldp statistic interface port-channel <port-list>	170
show logging	173
show logins	175
show loopguard	177
show mac address-table all [<sort>]	179
show mac address-table count	179
show mac address-table mac <mac-addr>	179
show mac address-table multicast	179
show mac address-table multicast	273
show mac address-table port <port-list> [<sort>]	179
show mac address-table static	179
show mac address-table vlan <vlan-list> [<sort>]	179
show mac-aging-time	179
show mac-authentication	181
show mac-authentication config	181
show memory	320
show mirror	188
show mrstp <tree-index>	191
show mstp	193
show mstp instance <number>	194
show multicast [vlan]	117
show multi-login	199
show mvr	201
show mvr <vlan-id>	201
show poe-status	213
show policy	217
show policy <name>	217
show port-access-authenticator	108
show port-access-authenticator <port-list>	108
show port-security	223
show port-security <port-list>	223
show power-source-status	320
show pppoe intermediate-agent	229
show pppoe intermediate-agent statistic	229
show pppoe intermediate-agent statistic vlan <vlan-list>	229
show private-vlan	234
show private-vlan <vlan-id>	234
show pwr	213
show radius-accounting	243
show radius-server	243
show remote-management [index]	245
show rmon alarm alarmtable [alarm-index]	250
show rmon event eventtable [event-index]	250
show rmon history historycontrol [index <historycontrol-index>]	250
show rmon history historycontrol port-channel <interface-id>	250
show rmon statistics etherstats [index <etherstats-index>]	250
show rmon statistics etherstats port-channel <interface-id>	250
show router dvmrp	83
show router igmp	112
show router ospf	205
show router ospf area	205
show router ospf network	205
show router ospf redistribute	205

show router ospf virtual-link	205
show router rip	247
show router vrrp	316
show running-config [interface port-channel <port-list> [<attribute> [<...>]]] ..	256
show running-config help	256
show running-config page	256
show service-control	245
show sflow	258
show sfp <port-list>	320
show slot	320
show slot config	320
show slot config <slot-list>	320
show smart-isolation	260
show snmp-server	263
show snmp-server [user]	264
show spanning-tree config	267
show ssh	271
show ssh key <rsa1 rsa dsa>	271
show ssh known-hosts	271
show ssh session	271
show subnet-vlan	279
show system-information	320
show tacacs-accounting	285
show tacacs-server	285
show time	67
show timesync	68
show trtcm dscp profile	293
show trunk	289
show version [flash]	320
show vlan	298
show vlan <vlan-id>	298
show vlan <vlan-id>	303
show vlan <vlan-id> counters	298
show vlan <vlan-id> interface port-channel <port-num> counters	298
show vlan1q gvrp	99
show vlan1q ingress-check	299
show vlan1q port-isolation	307
show vlan-stacking	309
shutdown slot <slot-list>	321
smart-isolation	260
snmp-server [<contact <system-contact>] [location <system-location>]>	263
snmp-server get-community <property>	263
snmp-server set-community <property>	263
snmp-server trap-community <property>	263
snmp-server trap-destination <ip> [udp-port <socket-number>] [version <v1 v2c v3>] [username <name>]	264
snmp-server trap-destination <ip> enable traps	264
snmp-server trap-destination <ip> enable traps aaa	264
snmp-server trap-destination <ip> enable traps aaa <options>	264
snmp-server trap-destination <ip> enable traps interface	265
snmp-server trap-destination <ip> enable traps interface <options>	265
snmp-server trap-destination <ip> enable traps ip	265
snmp-server trap-destination <ip> enable traps ip <options>	265
snmp-server trap-destination <ip> enable traps switch	265
snmp-server trap-destination <ip> enable traps switch <options>	265
snmp-server trap-destination <ip> enable traps system	265
snmp-server trap-destination <ip> enable traps system <options>	265
snmp-server username <name> sec-level <noauth auth priv> [auth <md5 sha> auth-password <password>] [priv <des aes> priv-password <password>] group <group-name> ..	264

snmp-server version <v2c v3 v3v2c>	263
source-port <port-list>	201
spanning-tree	267
spanning-tree <port-list>	267
spanning-tree <port-list> edge-port	268
spanning-tree <port-list> path-cost <1-65535>	268
spanning-tree <port-list> priority <0-255>	268
spanning-tree hello-time <1-10> maximum-age <6-40> forward-delay <4-30>	267
spanning-tree help	268
spanning-tree mode <RSTP MRSTP MSTP>	191
spanning-tree mode <RSTP MRSTP MSTP>	193
spanning-tree mode <RSTP MRSTP MSTP>	267
spanning-tree priority <0-61440>	267
speed-duplex <auto 10-half 10-full 100-half 100-full 1000-full>	126
spq	240
spq	242
ssh <1 2> <[user@]dest-ip> [command </>]	271
ssh known-hosts <host-ip> <1024 ssh-rsa ssh-dsa> <key>	271
storm-control	45
Subnet ID	140
subnet-based-vlan	279
subnet-based-vlan dhcp-vlan-override	279
subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> source-port <port> vlan <vlan-id> priority <0-7>	279
subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> vlan <vlan-id> pri- ority <0-7>	279
subnet-based-vlan name <name> source-ip <ip> mask-bits <mask-bits> vlan <vlan-id> pri- ority <0-7> inactive	279
sync running-config	256
syslog	281
syslog server <ip-address> inactive	281
syslog server <ip-address> level <level>	281
syslog type <type>	281
syslog type <type> facility <0-7>	281
tacacs-accounting host <index> <ip> [acct-port <socket-number>] [key <key-string>] ..	285
tacacs-accounting timeout <1-1000>	285
tacacs-server host <index> <ip> [auth-port <socket-number>] [key <key-string>] ..	285
tacacs-server mode <index-priority round-robin>	285
tacacs-server timeout <1-1000>	285
tagged <port-list>	201
test interface port-channel <port-list>	320
time <hour:min:sec>	67
time date <month/day/year>	67
time daylight-saving-time	67
time daylight-saving-time end-date <week> <day> <month> <o'clock>	68
time daylight-saving-time help	68
time daylight-saving-time start-date <week> <day> <month> <o'clock>	68
time timezone <-1200 ... 1200>	67
timesync <daytime time ntp>	68
timesync server <ip>	68
traceroute <ip host-name> [vlan <vlan-id>] [ttl <1-255>] [wait <1-60>] [queries <1-10>] 321	321
traceroute help	321
transceiver-ddm timer <1 - 4294967>	321
trtcm	293
trtcm	293
trtcm cir <rate>	294
trtcm dscp green <0-63>	294
trtcm dscp profile <name>	294

trtcm dscp profile <name> dscp green <0-63> yellow <0-63> red <0-63>	293
trtcm dscp red <0-63>	294
trtcm dscp yellow <0-63>	294
trtcm mode <color-aware color-blind>	293
trtcm pir <rate>	294
trunk <T1 T2 T3 T4 T5 T6>	289
trunk <T1 T2 T3 T4 T5 T6> criteria <src-mac dst-mac src-dst-mac src-ip dst-ip src-dst- ip>	289
trunk <T1 T2 T3 T4 T5 T6> interface <port-list>	289
trunk <T1 T2 T3 T4 T5 T6> lacp	289
trunk interface <port-list> timeout <lacp-timeout>	289
unknown-multicast-frame <drop flooding>	111
untagged <port-list>	298
vlan <1-4094>	303
vlan <1-4094>	319
vlan <vlan-id>	298
vlan1q gvrp	99
vlan1q ingress-check	299
vlan1q port-isolation	307
vlan-mapping	305
vlan-mapping name <name> interface port-channel <port> vlan <1-4094> translated-vlan <1- 4094> priority <0-7>	305
vlan-mapping name <name> interface port-channel <port> vlan <1-4094> translated-vlan <1- 4094> priority <0-7> inactive	305
vlan-stacking	309
vlan-stacking <sptpid>	310
vlan-stacking priority <0-7>	309
vlan-stacking role <normal access tunnel>	309
vlan-stacking selective-qinq name <name> interface port-channel <port> cvid <cvid> spvid <spvid> priority <0-7>	310
vlan-stacking selective-qinq name <name> interface port-channel <port> cvid <cvid> spvid <spvid> priority <0-7> inactive	310
vlan-stacking SPVID <1-4094>	309
vlan-stacking tunnel-tpid <tpid>	309
vlan-trunking	313
vlan-type <802.1q port-based>	225
vlan-type <802.1q port-based>	298
weight <wt1> <wt2> ... <wt8>	241
wfq	241
wfq	242
write memory [<index>]	321
wrr	241
wrr	242
wrr <wt1> <wt2> ... <wt8>	241

