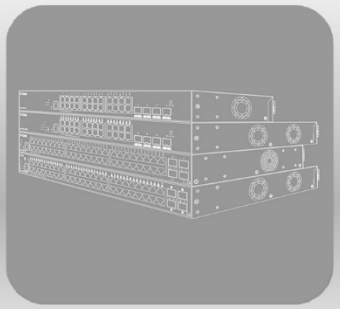
D-Link
Building Networks for People



CLI Reference Guide

Product Model: DXS-1210 Series

10 Gigabit Ethernet Smart Managed Switch

Release 1.00

Table of Contents

1. Introduction....1
2. Basic CLI Commands....7
3. 802.1X Commands....18
4. Access Control List (ACL) Commands....31
5. Access Management Commands....49
6. ARP Spoofing Prevention Commands....64
7. Asymmetric VLAN Commands....66
8. Authentication, Authorization, and Accounting (AAA) Commands....67
9. Basic IPv4 Commands....75
10. Basic IPv6 Commands....81
11. Cable Diagnostics Commands....95
12. Debug Commands....98
13. DHCP Auto-Configuration Commands....103
14. DHCP Auto-Image Commands....105
15. DHCP Client Commands....108
16. DHCP Relay Commands....111
17. DHCP Server Screening Commands....132
18. DHCP Snooping Commands....137
19. DHCPv6 Client Commands....154
20. DHCPv6 Guard Commands....156
21. DHCPv6 Relay Commands....160
22. D-Link Discovery Protocol (DDP) Client Commands....173
23. Domain Name System (DNS) Commands....178
24. DoS Prevention Commands....183
25. Dynamic ARP Inspection Commands....187
26. Error Recovery Commands....200
27. File System Commands....203
28. Filter Database (FDB) Commands....205
29. Gratuitous ARP Commands....217
30. Interface Commands....220
31. Internet Group Management Protocol (IGMP) Snooping Commands....241
32. IP-MAC-Port Binding (IMPB) Commands....256
33. IP Multicast (IPMC) Commands....260
34. IP Multicast Version 6 (IPMCv6) Commands....261
35. IP Source Guard Commands....262
36. IP Utility Commands....267
37. IPv6 Snooping Commands....270
38. IPv6 Source Guard Commands....275
39. Link Aggregation Control Protocol (LACP) Commands....281
40. Link Layer Discovery Protocol (LLDP) Commands....287
41. Loopback Detection (LBD) Commands....312

42. Mirror Commands....319
43. Multicast Listener Discovery (MLD) Snooping Commands....322
44. Multiple Spanning Tree Protocol (MSTP) Commands....337
45. Neighbor Discovery (ND) Inspection Commands....346
46. Network Access Authentication Commands....350
47. Network Protocol Port Protection Commands....359
48. Packet Debug Commands....361
49. Port Security Commands....364
50. Power Saving Commands....370
51. Protocol Independent Commands....375
52. Quality of Service (QoS) Commands....380
53. Remote Network MONitoring (RMON) Commands....402
54. Router Advertisement (RA) Guard Commands....409
55. Safeguard Engine Commands....413
56. Secure Shell (SSH) Commands....420
57. Simple Network Management Protocol (SNMP) Commands....427
58. Spanning Tree Protocol (STP) Commands....447
59. Storm Control Commands....460
60. Surveillance VLAN Commands....465
61. Switch Port Commands....476
62. System File Management Commands....480
63. System Log Commands....490
64. Time and SNTP Commands....498
65. Time Range Commands....504
66. Traffic Segmentation Commands....507
67. Transport Layer Security (TLS) Commands....509
68. Virtual LAN (VLAN) Commands....518
69. Voice VLAN Commands....527
Appendix A - System Log Entries....534
Appendix B - Trap Entries....552
Appendix C - RADIUS Attributes Assignment....559
Appendix D - IETF RADIUS Attributes Support....560

1. Introduction

This manual's command descriptions are based on the software release **1.00**. The commands listed here are the subset of commands that are supported by the DXS-1210 Series switch.

Audience

This reference manual is intended for network administrators and other IT networking professionals responsible for managing the switch by using the Command Line Interface (CLI). The CLI is one of the management interfaces to the DXS-1210 Series switch, which will be generally be referred to simply as the "Switch" within this manual. This manual is written in a way that assumes that you already have experience with and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

The documents below are a further source of information in regards to configuring and troubleshooting the Switch. All the documents are available from the D-Link website. Other documents related to this switch are:

- DXS-1210 Series Hardware Installation Guide
- DXS-1210 Series Web UI Reference Guide

Conventions

Convention	Description
Boldface Font	Commands, command options and keywords are printed in boldface. Keywords, in the command line, are to be entered exactly as they are displayed.
UPPERCASE ITALICS Font	Parameters or values that must be specified are printed in *UPPERCASE ITALICS*. Parameters in the command line are to be replaced with the actual values that are desired to be used with the command.
Square Brackets [ ]	Square brackets enclose an optional value or set of optional arguments.
Braces { }	Braces enclose alternative keywords separated by vertical bars. Generally, one of the keywords in the separated list can be chosen.
Vertical Bar |	Optional values or arguments are enclosed in square brackets and separated by vertical bars. Generally, one or more of the vales or arguments in the separated list can be chosen.
`Blue Courier Font`	This convention is used to represent an example of a screen console display including example entries of CLI command input with the corresponding output. All examples used in this manual are based on the DXS-1210-28T switch in the DXS-1210 Series.

Notes, Notices, and Cautions

Below are examples of the three types of indicators used in this manual. When administering your switch using the information in this document, you should pay special attention to these indicators. Each example below provides an explanatory remark regarding each type of indicator.

NOTE: A note indicates important information that helps you make better use of your device.

NOTICE: A notice indicates either potential damage to hardware or loss of data and tells you how to avoid the problem.

CAUTION: A caution indicates a potential for property damage, personal injury, or death.

Connecting to the Console Port

The Console port is used to connect to the CLI of the Switch. Connect the DB9 connector of the console cable (included in the packaging) to the Serial (COM) port of the computer. Connect the RJ45 connector of the console cable to the Console port on the Switch.

To access the CLI through the Console port, Terminal Emulation Software must be used like *PuTTY* or *Tera Term*. The Switch uses a connection of **115200** bits per second with **no flow control** enabled.

After the boot sequence completed, the CLI login screen is displayed.

Command Descriptions

The information pertaining to each command in this reference guide is presented using a number of template fields. The fields are:

- **Description** - This is a short and concise statement describing the functionality of the command.
- **Syntax** - The precise form to use when entering and issuing the command.
- **Parameters** - A table where each row describes the optional or required parameters, and their use, that can be issued with the command.
- **Default** - If the command sets a configuration value or administrative state of the Switch then any default settings (i.e. without issuing the command) of the configuration is shown here.
- **Command Mode** - The mode in which the command can be issued. These modes are described in the section titled “Command Modes” below.
- **Usage Guideline** - If necessary, a detailed description of the command and its various utilization scenarios is given here.
- **Example(s)** - Each command is accompanied by a practical example of the command being issued in a suitable scenario.

Command Modes

There are several command modes available in the command-line interface (CLI). The set of commands available to the user depends on the mode the user is currently in. The user can see all the commands that are available in a particular command mode by entering a question mark (?) at the system prompt.

The command-line interface has a number of command modes. There are three basic command modes:

- **EXEC Mode**
- **Global Configuration Mode**

All other sub-configuration modes can be accessed via the **Global Configuration Mode**.

EXEC Mode

Users logged in with this command mode can monitor all system information and change any system configuration settings mentioned in this Configuration Guide.

Global Configuration Mode

The primary purpose of the global configuration mode is to apply global settings to the entire switch. In addition to applying global settings to the entire switch, the user can also access other sub-configuration modes. In order to access the global configuration mode, enter the **configure terminal** command in the EXEC mode.

The following example shows how to enter the Global Configuration mode.

```
Switch# configure terminal
Switch(config)#
```

The **exit** command is used to exit the Global Configuration Mode and return to the EXEC Mode.

```
Switch(config)# exit
Switch#
```

The procedures to enter the different sub-configuration modes can be found in the related chapters in this Configuration Guide. The command modes are used to configure the individual functions.

Creating a User Account

You can create multiple user accounts. This section will assist a user with creating a user account by means of the Command Line Interface.

NOTE: By default, one user account is already configured on the Switch. Both the username and password for this account is **admin**.

Observe the following example.

```
Switch#configure terminal
Switch(config)#username account password account
```

In the above example we had to navigate and access the username command.

- We entered the **configure terminal** command to access the Global Configuration Mode. The **username** command can be used in the Global Configuration Mode.
- The **username account password account** command creates an account with the username of *account* and a password of *account*.

Save the running configuration to the start-up configuration. This means to save the changes made so that when the Switch is rebooted, the configuration will not be lost. The following example shows how to save the running configuration to the start-up configuration.

```
Switch# copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM..... Done.

Switch#
```

After the Switch has rebooted, or after the users log out and back in, the newly created username and password must be entered to access the CLI interface again, as seen below.

```
                DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch

                                Command Line Interface
                               Firmware: Build 1.00.021
             Copyright(C) 2020 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****
```

Error Messages

When users issue a command that the Switch does not recognize, error messages will be generated to assist users with basic information about the mistake that was made. A list of possible error messages are found in the table below.

Error Message	Meaning
Ambiguous command	Not enough keywords were entered for the Switch to recognize the command.
Incomplete command	The command was not entered with all the required keyword.
Invalid input detected at ^marker	The command was entered incorrectly.

The following example shows how an ambiguous command error message is generated.

```
Switch#show v
Ambiguous command
Switch#
```

The following example shows how an incomplete command error message is generated.

```
Switch#show
Incomplete command
Switch#
```

The following example shows how an invalid input error message is generated.

```
Switch#show verb
            ^
Invalid input detected at ^marker
Switch#
```

Editing Features

The command line interface of this switch supports the following keyboard keystroke editing features.

Keystroke	Description
Delete	Deletes the character under the cursor and shifts the remainder of the line to the left.

Backspace	Deletes the character to the left of the cursor and shifts the remainder of the line to the left.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
CTRL+R	Toggles the insert text function on and off. When on, text can be inserted in the line and the remainder of the text will be shifted to the right. When off, text can be inserted in the line and old text will automatically be replaced with the new text.
Return	Scrolls down to display the next line or used to issue a command.
Space	Scrolls down to display the next page.
ESC	Escapes from the displaying page.

Display Result Output Modifiers

Results displayed by **show** commands can be filtered using the following parameters:

- **begin** *FILTER-STRING* - This parameter is used to start the display with the first line that matches the filter string.
- **include** *FILTER-STRING* - This parameter is used to display all the lines that match the filter string.
- **exclude** *FILTER-STRING* - This parameter is used to exclude the lines that match the filter string from the display.

The example below shows how to use the **begin** *FILTER-STRING* parameter in a **show** command.

```
Switch#show running-config | begin line console
line console
 session-timeout 0
!
line telnet
!
line ssh
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
!
interface Ethernet1/0/3
!
interface Ethernet1/0/4
!
interface Ethernet1/0/5
!
interface Ethernet1/0/6
!
interface Ethernet1/0/7
!
interface Ethernet1/0/8
!
interface Ethernet1/0/9
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

The example below shows how to use the **include** *FILTER-STRING* parameter in a **show** command.

```
Switch#show running-config | include Firmware
!                           Firmware: Build 1.00.021


Switch#
```

The example below shows how to use the **exclude** *FILTER-STRING* parameter in a **show** command.

```
Switch#show running-config | exclude !
Building configuration...

Current configuration : 1416 bytes


ip http timeout-policy idle 36000
line console
 session-timeout 0
line telnet
line ssh
interface Ethernet1/0/1
interface Ethernet1/0/2
interface Ethernet1/0/3
interface Ethernet1/0/4
interface Ethernet1/0/5
interface Ethernet1/0/6
interface Ethernet1/0/7
interface Ethernet1/0/8
interface Ethernet1/0/9
interface Ethernet1/0/10
interface Ethernet1/0/11
interface Ethernet1/0/12
interface Ethernet1/0/13
interface Ethernet1/0/14
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

2. Basic CLI Commands

2-1 help

This command is used to display a brief description of the help system. Use the help command in any command mode.

help

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Any Configuration Mode.

Usage Guideline

This command provides a brief description for the help system, which includes the following functions:

- To list all commands available for a particular command mode, enter a question mark (?) at the system prompt.
- To obtain a list of commands that begin with a particular character string, enter the abbreviated command entry immediately followed by a question mark (?). This form of help is called **word** help, because it lists only the keywords or arguments that begin with the abbreviation entered.
- To list the keywords and arguments associated with a command, enter a question mark (?) in place of a keyword or argument on the command line. This form of help is called the **command syntax** help, because it lists the keywords or arguments that apply based on the command, keywords, and arguments already entered.

Example

This example shows how the help command is used to display a brief description of the help system.

```
Switch#help

The switch CLI provides advanced help feature.
1. Help is available when you are ready to enter a command
   argument (e.g. 'show ?') and want to know each possible
   available options.
2. Help is provided when an abbreviated argument is entered
   and you want to know what arguments match the input(e.g. 'show ve?'.).
   If nothing matches, the help list will be empty and you must backup
   until entering a '?' shows the available options.
3. For completing a partial command name could enter the abbreviated
   command name immediately followed by a <Tab> key.

Note:
Since the character '?' is used for help purpose, to enter
the character '?' in a string argument, press ctrl+v immediately
followed by the character '?'.

Switch#
```

The following example shows how to use the **word** help to display all the Privileged EXEC Mode commands that begin with the letters “re”. The letters entered before the question mark (?) are reprinted on the next command line to allow the user to continue entering the command.

```
Switch#re?
reboot  renew  reset

Switch#re
```

This example shows how to use the **command syntax** help to display the next argument of a partially complete **copy** command. The characters entered before the question mark (?) is reprinted on the next command line to allow the user to continue entering the command.

```
Switch#copy ?
  attack-log      Copy from attack log
  flash:          Copy from flash: file system
  log             Copy from log
  running-config  Copy from current system configuration
  startup-config  Copy from boot-up configuration
  tftp:           Copy from tftp: file system

Switch#copy
```

2-2 configure terminal

This command is used to enter the Global Configuration Mode.

configure terminal

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to enter the Global Configuration Mode.

Example

This example shows how to enter the Global Configuration Mode.

```
Switch# configure terminal
Switch(config)#
```

2-3 login (EXEC)

This command is used to configure a login username.

login

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to change the login account. Three attempts are allowed to login to the Switch's interface. When using Telnet, if all attempts fail, access will return to the command prompt. If no information is entered within 60 seconds, the session will return to the state when logged out.

Example

This example shows how to log in with username "user1".

```
Switch# login

Username: user1
Password: xxxxx

Switch#
```

2-4 logout

This command is used to close an active terminal session by logging off the Switch.

logout

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to close an active terminal session by logging off the Switch.

Example

This example shows how to log out.

```
Switch# logout
```

2-5 end

This command is used to end the current configuration mode and return to the highest mode in the CLI mode hierarchy which is EXEC Mode.

end

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Any Configuration Mode.

Usage Guideline

Use this command to return access to the highest mode in the CLI hierarchy regardless of what configuration mode or configuration sub-mode currently located at.

Example

This example shows how to end the Interface Configuration Mode and go back to the EXEC Mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)#end
Switch#
```

2-6 exit

This command is used to end the configuration mode and go back to the last mode. If the current mode is the EXEC Mode, executing the exit command logs you out of the current session.

exit

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Any Configuration Mode.

Usage Guideline

Use this command to exit the current configuration mode and go back to the last mode. When the user is in the User EXEC Mode or the Privileged EXEC Mode, this command will logout the session.

Example

This example shows how to exit from the Interface Configuration Mode and return to the Global Configuration Mode.

```
Switch# configure terminal
Switch(config) interface eth1/0/1
Switch(config-if)#exit
Switch(config)#
```

2-7 show history

This command is used to list the commands entered in the current EXEC Mode session.

show history

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Commands entered are recorded by the system. A recorded command can be recalled in sequence by pressing CTRL+P or the Up Arrow key. The history buffer size is fixed at 20 commands.

The function key instructions below display how to navigate the commands in the history buffer.

- CTRL+P or the Up Arrow key - Recalls commands in the history buffer, beginning with the most recent command. Repeat the key sequence to recall successively older commands.
- CTRL+N or the Down Arrow key - Returns to more recent commands in the history buffer after recalling commands with Ctrl-P or the Up Arrow key. Repeat the key sequence to recall successively more recent commands.

Example

This example shows how to display the command buffer history.

```
Switch#show history

 help
 history

Switch#
```

2-8 show environment

This command is used to display fan, temperature, power availability and status information.

show environment [fan | power | temperature]

Parameters

fan	(Optional) Specifies to display the Switch fan detailed status.
power	(Optional) Specifies to display the Switch power detailed status.
temperature	(Optional) Specifies to display the Switch temperature detailed status.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all types of environment information will be displayed.

Example

This example shows how to display fan, temperature, power availability, and status information.

```
Switch# show environment

Detail Temperature Status:
Temperature Descr/ID          Current/Threshold Range
------------------------------------------------------
Central Temperature/1         33C/11~79C
Status code: * temperature is out of threshold range

Detail Fan Status:
------------------------------------------------------------------
Right Fan 1 (OK)     Right Fan 2 (OK)

Detail Power Status:
Power Module      Power Status
---------------   -------------
Power 1           In-operation

Switch#
```

Display Parameters

Power status	• **In-operation** - The power rectifier is in normal operation. • **Failed** - The power rectifier not working normally. • **Empty** - The power rectifier is not installed.

2-9 show unit

This command is used to display information about system units.

show unit

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the system modules.

Example

This example shows how to display the information about system units.

```
Switch#show unit

Model Descr: 24P 10GBASE-T with 4P 25G SFP28
Model Name: DXS-1210-28T
Serial-Number: DXS1210102030
Status: OK
Up Time: 0DT1H30M18S
DRAM      255264 K total,   206868 K used,    48396 K free
FLASH      64640 K total,    38596 K used,    26044 K free

Switch#
```

2-10 show cpu utilization

This command is used to display the CPU utilization information.

show cpu utilization

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the CPU utilization information of the Switch in 5 second, 1 minute, and 5 minute intervals.

Example

This example shows how to display the information about CPU utilization.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -   3 %         One minute -   3 %         Five minutes -   4 %


Switch#
```

2-11 show version

This command is used to display the version information of the Switch.

show version

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the version information of the Switch.

Example

This example shows how to display the version information of the Switch.

```
Switch#show version

System MAC Address: F0-7D-68-12-10-01

  Module Name: DXS-1210-28T
  H/W: A1
  Runtime: 1.00.021

Switch#
```

2-12 snmp-server enable traps environment

This command is used to enable the power, temperature and fan trap states. Use the **no** form of this command to disable the state.

snmp-server enable traps environment [fan] [power] [temperature]

no snmp-server enable traps environment [fan] [power] [temperature]

Parameters

fan	(Optional) Specifies to enable or disable the Switch's fan trap state for warning fan events (fan failed or fan recover).
power	(Optional) Specifies to enable or disable the Switch's power trap state for warning power events (power failure or power recovery).
temperature	(Optional) Specifies to enable or disable the Switch's temperature trap state for warning temperature events (temperature exceeds the thresholds or temperature recover).

Default

By default, all environment device traps are disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the environment trap states for fan, power and temperature events. If no parameter is specified, all of the environment traps are enabled or disabled.

Example

This example shows how to enable the environment trap status..

```
Switch# configure terminal
Switch(config)# snmp-server enable traps environment
Switch(config)#
```

2-13 environment temperature threshold

This command is used to configure the environment temperature thresholds. Use the **no** form of this command to revert to the default setting.

environment temperature threshold thermal [high *VALUE*] **[low** *VALUE*]

no environment temperature threshold thermal [high] [low]

Parameters

high	(Optional) Specifies the high threshold of the temperature in Celsius. The range is from -100 to 200.
low	(Optional) Specifies the low threshold of the temperature in Celsius. The range is from -100 to 200. The low threshold must be smaller than the high threshold.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the environment temperature threshold which corresponds to the normal range of the temperature defined for the sensor. The low threshold must be smaller than the high threshold. The configured range must fall within the operational range which corresponds to the minimum and maximum allowed temperatures defined for the sensor. When the configured threshold is crossed, a notification will be sent.

Example

This example shows how to configure the environment temperature thresholds.

```
Switch# configure terminal
Switch(config)#environment temperature threshold thermal high 100 low 20
Switch(config)#
```

2-14 show memory utilization

This command is used to display the memory utilization information.

show memory utilization

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the memory utilization information of the Switch including DRAM and flash.

Example

This example shows how to display the information about memory utilization.

```
Switch#show memory utilization

DRAM      255264 K total,   206868 K used,    48396 K free
FLASH      64640 K total,    38596 K used,    26044 K free

Switch#
```

3. 802.1X Commands

3-1 clear dot1x counters

This command is used to clear 802.1X counters (diagnostics, statistics, and session statistics).

clear dot1x counters {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear 802.1X counters (diagnostics, statistics and session statistics) on all interfaces.
interface *INTERFACE-ID*	Specifies to clear 802.1X counters (diagnostics, statistics and session statistics) on the specified interface. Valid interfaces are physical ports (including type and port number).
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear 802.1X counters (diagnostics, statistics and session statistics).

Example

This example shows how to clear 802.1X counters (diagnostics, statistics and session statistics) on port 1.

```
Switch# clear dot1x counters interface eth1/0/1
Switch#
```

3-2 dot1x control-direction

This command is used to configure the direction of the traffic on a controlled port as unidirectional (in) or bidirectional (both). Use the **no** form of this command to revert to the default setting.

dot1x control-direction {both | in}

no dot1x control-direction

Parameters

both	Specifies to enable bidirectional control for the port.
in	Specifies to enable in direction control for the port.

Default

By default, this option is bidirectional mode.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration. If the port control is set to **force-authorized**, then the port is not controlled in both directions. If the port control is set to **auto**, the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, the access to the port for the controlled direction is blocked.

Suppose that port control is set to **auto**. If the control direction is set to **both**, the port can receive and transmit EAPOL packets only. All user traffic is blocked before authentication. If the control direction is set to in, in addition to receiving and transmitting EAPOL packets, the port can transmit user traffic but not receive user traffic before authentication. The **in** control direction is only valid when the **multi-host** mode is configured using the **authentication host-mode** command.

Example

This example shows how to configure the controlled direction of the traffic on port 1 as unidirectional.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x control-direction in
Switch(config-if)#
```

3-3 dot1x default

This command is used to reset the IEEE 802.1X parameters on a specific port to their default settings.

dot1x default

Parameters

None.

Default

IEEE 802.1X authentication is disabled.

Control direction is bidirectional (both).

Port control is auto.

Forward PDU on port is disabled.

Maximum request is 2 times.

Server timer is 30 seconds.

Supplicant timer is 30 seconds.

Transmit interval is 30 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to reset all the IEEE 802.1X parameters on a specific port to their default settings.

Example

This example shows how to reset the 802.1X parameters on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x default
Switch(config-if)#
```

3-4 dot1x port-control

This command is used to control the authorization state of a port. Use the **no** form of this command to revert to the default setting.

dot1x port-control {auto | force-authorized | force-unauthorized}

no dot1x port-control

Parameters

auto	Specifies to enable IEEE 802.1X authentication for the port.
force-authorized	Specifies the port to the force authorized state.
force-unauthorized	Specifies the port to the force unauthorized state.

Default

By default, this option is set as **auto**.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

This command takes effect only when IEEE 802.1X PAE authenticator is globally enabled by the **dot1x system-auth-contro**l command and is enabled for a specific port by using the dot1x PAE authenticator.

If the port control is set to **force-authorized**, the port is not controlled in both directions. If the port control is set to **auto**, the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, the access to the port for the controlled direction is blocked.

Example

This example shows how to deny all access on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x port-control force-unauthorized
Switch(config-if)#
```

3-5 dot1x forward-pdu

This command is used to enable the forwarding of the dot1x PDU. Use the **no** form of this command to disable the forwarding of the dot1x PDU.

dot1x forward-pdu

no dot1x forward-pdu

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration. This command only takes effect when the dot1x authentication function is disabled on the receipt port. The received PDU will be forwarded in either the tagged or untagged form based on the VLAN setting.

Example

This example shows how to configure the forwarding of the dot1x PDU.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x forward-pdu
Switch(config-if)#
```

3-6 dot1x initialize

This command is used to initialize the authenticator state machine on a specific port or associated with a specific MAC address.

dot1x initialize {interface *INTERFACE-ID* **[, | -] | mac-address** *MAC-ADDRESS***}**

Parameters

interface *INTERFACE-ID*	Specifies the port on which the authenticator state machine will be initialized. Valid interfaces are physical ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
mac-address *MAC-ADDRESS*	Specifies the MAC address to be initialized.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

In the multi-host mode, specify an interface ID to initialize a specific port.

In the multi-auth mode, specify a MAC address to initialize a specific MAC address.

Example

This example shows how to initialize the authenticator state machine on port 1.

```
Switch# dot1x initialize interface eth1/0/1
Switch#
```

3-7 dot1x max-req

This command is used to configure the maximum number of times that the backend authentication state machine will retransmit an Extensible Authentication Protocol (EAP) request frame to the supplicant before restarting the authentication process. Use the **no** form of this command to revert to the default setting.

dot1x max-req *TIMES*

no dot1x max-req

Parameters

TIMES	Specifies the number of times that the Switch retransmits an EAP frame to the supplicant before restarting the authentication process. The range is 1 to 10.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Usage Guideline

The command is only available for physical port interface configuration. If no response to an authentication request from the supplicant within the timeout period (specified by the **dot1x timeout tx-period** *SECONDS* command), the Switch will retransmit the request. This command is used to specify the number of retransmissions.

Example

This example shows how to configure the maximum number of retries on port 1 to be 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x max-req 3
Switch(config-if)#
```

3-8 dot1x pae authenticator

This command is used to configure a specific port as an IEEE 802.1X port access entity (PAE) authenticator. Use the **no** form of this command to disable the port as an IEEE 802.1X authenticator.

dot1x pae authenticator

no dot1x pae authenticator

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration. Globally enable IEEE 802.1X authentication on the Switch by using the **dot1x system-auth-control** command. When IEEE 802.1X authentication is enabled, the system will authenticate the 802.1X user based on the method list configured by the **aaa authentication dot1x default** command.

Example

This example shows how to configure port 1 as an IEEE 802.1X PAE authenticator.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x pae authenticator
Switch(config-if)#
```

This example shows how to disable IEEE 802.1X authentication on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no dot1x pae authenticator
Switch(config-if)#
```

3-9 dot1x re-authenticate

This command is used to re-authenticate a specific port or a specific MAC address.

dot1x re-authenticate {interface *INTERFACE-ID* **[, | -] | mac-address** *MAC-ADDRESS***}**

Parameters

interface *INTERFACE-ID*	Specifies the port to re-authenticate. Valid interfaces are physical ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

mac-address *MAC-ADDRESS*	Specifies the MAC address to re-authenticate.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is used to re-authenticate a specific port or a specific MAC address.

In the multi-host mode, specify an interface ID to re-authenticate a specific port.

In the multi-auth mode, specify a MAC address to re-authenticate a specific MAC address.

Example

This example shows how to re-authenticate port 1.

```
Switch# dot1x re-authenticate interface eth1/0/1
Switch#
```

3-10 dot1x system-auth-control

This command is used to globally enable IEEE 802.1X authentication on the Switch. Use the **no** form of this command to disable IEEE 802.1X authentication.

dot1x system-auth-control

no dot1x system-auth-control

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The 802.1X authentication function restricts unauthorized hosts from accessing the network. Use the **dot1x system-auth-control** command to globally enable the 802.1X authentication control. When 802.1X authentication is enabled, the system will authenticate the 802.1X user based on the method list configured by the **aaa authentication dot1x default** command.

Example

This example shows how to enable IEEE 802.1X authentication globally on the Switch.

```
Switch# configure terminal
Switch(config)# dot1x system-auth-control
Switch(config)#
```

3-11 dot1x timeout

This command is used to configure IEEE 802.1X timers. Use the **no** form of this command to revert to the default settings.

dot1x timeout {server-timeout *SECONDS* **| supp-timeout** *SECONDS* **| tx-period** *SECONDS***}**

no dot1x timeout {server-timeout | supp-timeout | tx-period}

Parameters

server-timeout *SECONDS*	Specifies the number of seconds that the Switch will wait for the request from the authentication server before timing out the server. On timeout, the authenticator will send an EAP-Request packet to the client. The range is 1 to 65535.
supp-timeout *SECONDS*	Specifies the number of seconds that the Switch will wait for the response from the supplicant before timing out supplicant messages other than the EAP request ID. The range is 1 to 65535.
tx-period *SECONDS*	Specifies the number of seconds that the Switch will wait for a response to an EAP-Request/Identity frame from the supplicant before retransmitting the request. The range is 1 to 65535.

Default

The **server-timeout** is 30 seconds.

The **supp-timeout** is 30 seconds.

The **tx-period** is 30 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Example

This example shows how to configure the server timeout value, supplicant timeout value, and the TX period on port 1 to be 15, 15, and 10 seconds, respectively.

```
configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# dot1x timeout server-timeout 15
Switch(config-if)# dot1x timeout supp-timeout 15
Switch(config-if)# dot1x timeout tx-period 10
Switch(config-if)#
```

3-12 show dot1x

This command is used to display the IEEE 802.1X global configuration or interface configuration.

show dot1x [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x configuration on the specified interface or range of interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the global configuration or interface configuration. If no parameter is specified, the global configuration will be displayed.

Example

This example shows how to display the dot1X global configuration..

```
Switch# show dot1x

802.1X                       : Enabled
Trap State                   : Enabled

Switch#
```

This example shows how to display the dot1X configuration on port 1.

```
show dot1x interface eth1/0/1

Interface                  : eth1/0/1
PAE                        : Authenticator
Control Direction          : Both
Port Control               : Auto
Tx Period                  : 30 sec
Supp Timeout               : 30 sec
Server Timeout             : 30 sec
Max-req                    : 2 times
Forward PDU                : Disabled

Switch#
```

3-13 show dot1x diagnostics

This command is used to display IEEE 802.1X diagnostics.

show dot1x diagnostics [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display 802.1X diagnostics. If no parameter is specified, information of all interfaces will be displayed.

Example

This example shows how to display the dot1X diagnostics on port 1.

```
Switch# show dot1x diagnostics interface eth1/0/1

eth1/0/1 dot1x diagnostic information are following:
EntersConnecting                      : 20
EAP-LogoffsWhileConnecting            : 0
EntersAuthenticating                  : 0
SuccessesWhileAuthenticating          : 0
TimeoutsWhileAuthenticating           : 0
FailsWhileAuthenticating              : 0
ReauthsWhileAuthenticating            : 0
EAP-StartsWhileAuthenticating         : 0
EAP-LogoffsWhileAuthenticating        : 0
ReauthsWhileAuthenticated             : 0
EAP-StartsWhileAuthenticated          : 0
EAP-LogoffsWhileAuthenticated         : 0
BackendResponses                      : 0
BackendAccessChallenges               : 0
BackendOtherRequestsToSupplicant      : 0
BackendNonNakResponsesFromSupplicant  : 0
BackendAuthSuccesses                  : 0
BackendAuthFails                      : 0

Switch#
```

3-14 show dot1x statistics

This command is used to display IEEE 802.1X statistics.

show dot1x statistics [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display 802.1X statistics. If no parameter is specified, information of all interfaces will be displayed.

Example

This example shows how to display dot1X statistics on port 1.

```
Switch# show dot1x statistics interface eth1/0/1

eth1/0/1 dot1x statistics information:
EAPOL Frames RX                : 1
EAPOL Frames TX                : 4
EAPOL-Start Frames RX          : 0
EAPOL-Req/Id Frames TX         : 6
EAPOL-Logoff Frames RX         : 0
EAPOL-Req Frames TX            : 0
EAPOL-Resp/Id Frames RX        : 0
EAPOL-Resp Frames RX           : 0
Invalid EAPOL Frames RX        : 0
EAP-Length Error Frames RX     : 0
Last EAPOL Frame Version       : 0
Last EAPOL Frame Source        : 00-10-28-00-19-78

Switch#
```

3-15 show dot1x session-statistics

This command is used to IEEE 802.1X session statistics.

show dot1x session-statistics [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display 802.1X statistics. If no parameter is specified, information of all interfaces will be displayed.

Example

This example shows how to display dot1X statistics on port 1.

```
Switch# show dot1x session-statistics interface eth1/0/1

Eth1/0/1 session statistic counters are following:
SessionOctetsRX                       : 0
SessionOctetsTX                       : 0
SessionFramesRX                       : 0
SessionFramesTX                       : 0
SessionId                             :
SessionAuthenticationMethod           : Remote Authentication Server
SessionTime                           : 0
SessionTerminateCause                 : SupplicantLogoff
SessionUserName                       :

Switch#
```

3-16 snmp-server enable traps dot1x

This command is used to enable the sending of SNMP notifications for 802.1X authentication. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps dot1x

no snmp-server enable traps dot1x

Parameters

None.

Default

this feature is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for 802.1X authentication.

Example

This example shows how to enable the sending of traps for 802.1X authentication.

```
configure terminal
Switch(config)# snmp-server enable traps dot1x
Switch(config)#
```

4. Access Control List (ACL) Commands

4-1 access-list resequence

This command is used to re-sequence the starting sequence number and the increment number of the access list entries in an access list. Use the **no** form of this command to revert to the default setting.

access-list resequence {*NAME* **|** *NUMBER***}** *STARTING-SEQUENCE-NUMBER INCREMENT*

no access-list resequence

Parameters

NAME	Specifies the name of the access list to be configured. It can be a maximum of 32 characters.
NUMBER	Specifies the number of the access list to be configured.
STARTING-SEQUENCE-NUMBER	Specifies that the access list entries will be re-sequenced using this initial value. The default value is 10. The range of possible sequence numbers is 1 through 65535.
INCREMENT	Specifies the number that the sequence numbers step. The default value is 10. For example, if the increment (step) value is 5 and the beginning sequence number is 20, the subsequent sequence numbers are 25, 30, 35, 40, and so on. The range of valid values is from 1 to 32.

Default

The default start sequence number is 10.

The default increment is 10.

Command Mode

Global Configuration Mode.

Usage Guideline

This feature allows the user to re-sequence the entries of a specified access list with an initial sequence number determined by the *STARTING-SEQUENCE-NUMBER* parameter and continuing in the increments determined by the *INCREMENT* parameter. If the highest sequence number exceeds the maximum possible sequence number, there will be no re-sequencing.

If a rule entry is created without specifying the sequence number, the sequence number will be automatically assigned. If it is the first entry, a start sequence number is assigned. Subsequent rule entries are assigned a sequence number that is an increment value greater than the largest sequence number in that access list and the entry is placed at the end of the list.

After the start sequence number or increment change, the sequence number of all previous rules (include the rules that assigned sequence by user) will change according to the new sequence setting.

Example

This example shows how to re-sequence the sequence number of an IP access-list, named R&D.

```
Switch# show access-list ip R&D

Extended IP access list R&D(ID: 3552)
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

Switch# configure terminal
Switch(config)#ip access-list extended R&D
Switch(config-ip-ext-acl)# 5 permit tcp any 10.30.0.0 0.0.255.255
Switch(config-ip-ext-acl)# end
Switch# show access-list ip R&D

Extended IP access list R&D(ID: 3552)
     5 permit tcp any 10.30.0.0 0.0.255.255
     10 permit tcp any 10.20.0.0 0.0.255.255
     20 permit tcp any host 10.100.1.2
     30 permit icmp any any

Switch# configure terminal
Switch(config)# access-list resequence R&D 1 2
Switch(config)# exit
Switch# show access-list ip R&D

     Extended IP access list R&D(ID: 3552)
     1 permit tcp any 10.30.0.0 0.0.255.255
     3 permit tcp any 10.20.0.0 0.0.255.255
     5 permit tcp any host 10.100.1.2
     7 permit icmp any any

Switch#
```

4-2 acl-hardware-counter

This command is used to enable the ACL hardware counter of the specified access-list name for access group functions. Use the **no** form of this command to disable the ACL hardware counter function.

acl-hardware-counter access-group {*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***}**

no acl-hardware-counter access-group {A*CCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***}**

Parameters

access-group *ACCESS-LIST-NAME*	Specifies the name of the access list to be configured.
access-group *ACCESS-LIST-NUMBER*	Specifies the number of the access list to be configured.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the ACL hardware counter for all ports that have applied the specified access-list name or number. The number of packets that match each rule are counted.

Example

This example shows how to enable the ACL hardware counter.

```
configure terminal
Switch(config)# acl-hardware-counter access-group abc
Switch(config)#
```

4-3 clear acl-hardware-counter

This command is used to clear the ACL hardware counter.

clear acl-hardware-counter access-group [*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***]**

Parameters

access-group	Specifies access groups to be cleared.
ACCESS-LIST-NAME	(Optional) Specifies the name of the access list to be cleared.
ACCESS-LIST-NUMBER	(Optional) Specifies the number of the access list to be cleared.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all access-group hardware counters will be cleared.

Example

This example shows how to clear the ACL hardware counter.

```
Switch# clear acl-hardware-counter access-group abc
Switch#
```

4-4 ip access-group

This command is used to specify the IP access list to be applied to an interface. Use the **no** form of this command to remove an IP access list.

ip access-group {*NAME* **|** *NUMBER***} [in | out]**

no ip access-group [*NAME* **|** *NUMBER***] [in | out]**

Parameters

NAME	Specifies the name of the IP access-list to be applied. The name can be up to 32 characters.
NUMBER	Specifies the number of the IP access list to be applied.
in	(Optional) Specifies that the IP access list will be applied to check packets in the ingress direction. If the direction is not specified, **in** is used.
out	(Optional) Specifies that the IP access list will be applied to check packets in the egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

If an IP access group is already configured on the interface, the command applied later will overwrite the previous setting. Only one access list of the same type can be applied to the same interface; but access lists of different types can be applied to the same interface.

The association of an access group with an interface will consume the filtering entry resource in the Switch controller. If the resources are insufficient to commit the command, an error message will be displayed. There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, an error message will be displayed.

Example

This example shows how to specify the IP access list “Strict-Control” as an IP access group for port 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#ip access-group Strict-Control

PROMPT: The remaining applicable IP related access entries are 1536, remaining range entries
are 32.
Switch(config-if)#
```

4-5 ip access-list

This command is used to create or modify an IP access list. This command will enter into the IP Access-list Configuration Mode. Use the **no** form of this command to remove an IP access list.

ip access-list [extended] *NAME* **[***NUMBER***]**

no ip access-list [extended] {*NAME* **|** *NUMBER***}**

Parameters

extended	(Optional) Specifies that the IP access list is the extended IP access list, and more fields can be chosen for the filter. If the parameter is not specified, the IP access list is the standard IP access list.
NAME	Specifies the name of the IP access list to be configured. The maximum length is 32 characters. The first character must be a letter.

NUMBER	Specifies the ID number of the IP access list. For standard IP access lists, this value is from 1 to 1999. For extended IP access lists, this value is from 2000 to 3999.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of IP access list numbers will be assigned automatically.

Example

This example shows how to configure an extended IP access list, named “Strict-Control” and an IP access-list, named “pim-srcfilter”.

```
Switch# configure terminal
Switch(config)# ip access-list extended Strict-Control
Swtich(config-ip-ext-acl)# permit tcp any 10.20.0.0 0.0.255.255
Swtich(config-ip-ext-acl)# exit
Swtich(config)# ip access-list pim-srcfilter
Switch(config-ip-acl)# permit host 172.16.65.193 any
Switch(config-ip-acl)#
```

4-6 ipv6 access-group

This command is used to specify the IPv6 access list to be applied to an interface. Use the **no** form of this command to remove an IPv6 access list.

Ipv6 access-group {*NAME* **|** *NUMBER***} [in | out]**

no ipv6 access-group [*NAME* **|** *NUMBER***] [in | out]**

Parameters

NAME	Specifies the name of the IPv6 access-list to be applied. The name can be up to 32 characters.
NUMBER	Specifies the number of the IPv6 access list to be applied.
in	(Optional) Specifies that the IPv6 access list will be applied to check packets in the ingress direction. If the direction is not specified, **in** is used.
out	(Optional) Specifies that the IPv6 access list will be applied to check packets in the egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface. The association of an access group with an interface will consume the filtering entry resource in the switch controller. If the resource is insufficient to commit the command, an error message will be displayed.

There is a limitation on the number of port operator resources. If applying the command exhausts the available port selectors, an error message will be displayed.

Example

This example shows how to specify the IPv6 access list “ip6-control”as an IP access group on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 access-group ip6-control in

PROMPT: The remaining applicable IPv6 related access entries are 511, remaining range entr
ies are 32.
Switch(config-if)#
```

4-7 ipv6 access-list

This command is used to create or modify an IPv6 access list. This command will enter into IPv6 Access-list Configuration Mode. Use the **no** form of this command to remove an IPv6 access list.

ipv6 access-list [extended] *NAME* **[***NUMBER***]**

no ipv6 access-list [extended] {*NAME* **|** *NUMBER***}**

Parameters

extended	(Optional) Specifies that the IPv6 access list is the extended IPv6 access list, and more fields can be chosen for the filter. If the parameter is not specified, the IPv6 access list is the standard IPv6 access list.
NAME	Specifies the name of the IPv6 access list to be configured. The maximum length is 32 characters.
NUMBER	Specifies the ID number of the IPv6 access list. For standard IPv6 access lists, this value is from 11000 to 12999. For extended IPv6 access lists, this value is from 13000 to 14999.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The name must be unique among all access lists. The characters used in the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the IPv6 access list numbers will be assigned automatically.

Example

This example shows how to configure an extended IPv6 access list, named “ip6-control”.

```
Switch# configure terminal
Switch(config)# ipv6 access-list extended ip6-control
Swtich(config-ipv6-ext-acl)# permit tcp any 2002:f03::1/16
Switch(config-ipv6-ext-acl)#
```

This example shows how to configure an IPv6 standard access list, named “ip6-std-control”.

```
Switch# configure terminal
Switch(config)# ipv6 access-list ip6-std-control
Swtich(config-ipv6-acl)# permit any fe80::101:1/54
Switch(config-ipv6-acl)#
```

4-8 list-remark

This command is used to add remarks for the specified ACL. Use the **no** form of this command to delete the remarks.

list-remark *TEXT*

no list-remark

Parameters

TEXT	Specifies the remark information. The information can be up to 256 characters long.

Default

None.

Command Mode

Access-list Configuration Mode.

Usage Guideline

This command is available in the MAC, IP, and IPv6 Configure Mode.

Example

This example shows how to add a remark to the access-list.

```
Switch# configure terminal
Switch(config)# ip access-list extended R&D
Switch(config-ip-ext-acl)# list-remark This access-list is used to match any IP packets from
the host 10.2.2.1.
Switch(config-ip-ext-acl)# end
Switch# show access-list ip

Extended IP access list R&D(ID: 3999)
  10 permit host 10.2.2.1 any
  This access-list is used to match any IP packets from the host 10.2.2.1.

Switch#
```

4-9 mac access-group

This command is used to specify a MAC access list to be applied to an interface. Use the **no** form of this command to remove the access group control from the interface.

mac access-group {*NAME* **|** *NUMBER***} [in | out]**

no mac access-group [*NAME* **|** *NUMBER***] [in | out]**

Parameters

NAME	Specifies the name of the MAC access list to be applied.
NUMBER	Specifies the number of the MAC access list to be applied.
in	(Optional) Specifies that the MAC access list will be applied to check in the ingress direction. If direction is not specified, **in** is used.
out	(Optional) Specifies that the MAC access list will be applied to check packets in the egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

If MAC access group is already configured on the interface, the command applied later will overwrite the previous setting. MAC access-groups will only check non-IP packets.

Only one access list of the same type can be applied to the same interface, but access lists of different types can be applied to the same interface.

The association of an access group with an interface will consume the filtering entry resource in the switch controller. If the resource is insufficient to commit the command, an error message will be displayed.

Example

This example shows how to apply the MAC access list daily-profile to port 4.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#mac access-group daily-profile in

PROMPT: The remaining applicable MAC related access entries are 896, remaining range entri
es are 32.
Switch(config-if)#
```

4-10 mac access-list

This command is used to create or modify an MAC access list and this command will enter the MAC Access-list Configuration Mode. Use the **no** form of this command to delete a MAC access list.

mac access-list extended *NAME* **[***NUMBER***]**

no mac access-list extended {*NAME* **|** *NUMBER***}**

Parameters

NAME	Specifies the name of the MAC access list to be configured. The maximum length is 32 characters.
NUMBER	Specifies the ID number of the MAC access list. For extended MAC access lists, this value is from 6000 to 7999.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the MAC Access-list Configuration Mode, and use the **permit** or **deny** command to specify the entries. The name must be unique among all access lists. The characters of the name are case sensitive. If the access list number is not specified, the biggest unused number in the range of the MAC access list numbers will be assigned automatically.

Example

This example shows how to enter the MAC Access-list Configuration Mode for a MAC access list named “daily-profile”.

```
Switch# configure terminal
Switch(config)# mac access-list extended daily-profile
Switch(config-mac-ext-acl)#
```

4-11 permit | deny (ip access-list)

This command is used to add a permit or deny entry. Use the **no** form of this command to remove an entry.

Extended Access List:

[*SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} udp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} icmp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD}* **{any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [***ICMP-TYPE* **[***ICMP-CODE***] |** *ICMP-MESSAGE***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {gre | esp | eigrp | igmp | ipinip | ospf | pcp | pim | vrrp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***] [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

Standard IP Access List:

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IP-ADDR* **| S***RC-IP-ADDR SRC-IP-WILDCARD***} [any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Parameters

SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source IP address or any destination IP address.
host *SRC-IP-ADDR*	Specifies a specific source host IP address.
SRC-IP-ADDR SRC-IP-WILDCARD	Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-IP-ADDR*	Specifies a specific destination host IP address.
DST-IP-ADDR DST-IP-WILDCARD	Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
precedence *PRECEDENCE*	(Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7.
MASK	(Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
dscp *DSCP*	(Optional) Specifies the matching DSCP code in IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.

MASK	(Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if fall within the range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
fragments	(Optional) Specifies the packet fragment's filtering.
time-range *PROFILE-NAME*	(Optional) Specifies the name of the time period profile associated with the access list delineating its activation period.
tcp, udp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp	Specifies Layer 4 protocols.
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255.
MASK	(Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.
ICMP-CODE	(Optional) Specifies the ICMP message code. The valid number for the message code is from 0 to 255.
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The pre-defined parameters are available for selection: administratively-prohibited,alternate-address,conversion-error,host-prohibited,net-prohibited,echo,echo-reply,pointer-indicates-error,host-isolated,host-precedence-violation,host-redirect,host-tos-redirect,host-tos-unreachable,host-unknown,host-unreachable, information-reply,information-request,mask-reply,mask-request,mobile-redirect,net-redirect,net-tos-redirect,net-tos-unreachable, net-unreachable,net-unknown,bad-length,option-missing,packet-fragment,parameter-problem,port-unreachable,precedence-cutoff, protocol-unreachable,reassembly-timeout,redirect-message,router-advertisement,router-solicitation,source-quench,source-route-failed, time-exceeded,timestamp-reply,timestamp-request,traceroute,ttl-expired,unreachable.

Default

None.

Command Mode

IP Access-list Configuration Mode.

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the command access-list sequence to change the start sequence number and increment number for the specified access list. After the command is applied, the new rule without specified sequence number will be assigned sequence based new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will create extra effort to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access-list. If you enter a sequence number that is already present, an error message will be shown.

To create a matching rule for an IP standard access list, only the source IP address or destination IP address fields can be specified.

The VLAN range and the TCP/UDP port range can only be assigned to an ingress interface.

Example

This example shows how to create four entries for an IP extended access list, named Strict-Control. These entries are: permit TCP packets destined to network 10.20.0.0, permit TCP packets destined to host 10.100.1.2, permit all TCP packets go to TCP destination port 80 and permit all ICMP packets.

```
Switch# configure terminal
Switch(config)#ip access-list extended Strict-Control
Switch(config-ip-ext-acl)#permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)#permit tcp any host 10.100.1.2
Switch(config-ip-ext-acl)#permit tcp any any eq 80
Switch(config-ip-ext-acl)#permit icmp any any
Switch(config-ip-ext-acl)#
```

This example shows how to create two entries for an IP standard access-list, named “std-acl”. These entries are: permit IP packets destined to network 10.20.0.0, permit IP packets destined to host 10.100.1.2.

```
Switch# configure terminal
Switch(config)#ip access-list std-acl
Switch(config-ip-acl)#permit any 10.20.0.0 0.0.255.255
Switch(config-ip-acl)#permit any host 10.100.1.2
Switch(config-ip-acl)#
```

4-12 permit | deny (ipv6 access-list)

This command is used to add a permit entry or deny entry to the IPv6 access list. Use the **no** form of this command to remove an entry from the IPv6 access list.

Extended IPv6 Access List:

[*SEQUENCE-NUMBER***] {permit | deny} tcp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} udp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDR/PREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} icmp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [***ICMP-TYPE* **[***ICMP-CODE***] |** *ICMP-MESSAGE***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {esp | pcp | sctp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-*

ADDRIPREFIX-LENGTH} [**fragments**] [**dscp** *VALUE* [*MASK*] | **traffic-class** *VALUE* [**MASK**]] [**flow-label** *FLOW-LABEL* [*MASK*]] [**time-range** *PROFILE-NAME*]

[*SEQUENCE-NUMBER*] {**permit** | **deny**} {**any** | **host** *SRC-IPV6-ADDR* | *SRC-IPV6-ADDRIPREFIX-LENGTH*} [**any** | **host** *DST-IPV6-ADDR* | *DST-IPV6-ADDRIPREFIX-LENGTH*] [**fragments**] [**dscp** *VALUE* [*MASK*] | **traffic-class** *VALUE* [*MASK*]] [**flow-label** *FLOW-LABEL* [*MASK*]] [**time-range** *PROFILE-NAME*]

Standard IPv6 Access List:

[*SEQUENCE-NUMBER*] {**permit** | **deny**} {**any** | **host** *SRC-IPV6-ADDR* | *SRC-IPV6-ADDR/PREFIX-LENGTH*} [**any** | **host** *DST-IPV6-ADDR* | *DST-IPV6-ADDR/PREFIX-LENGTH*] [**time-range** *PROFILE-NAME*]

no *SEQUENCE-NUMBER*

Parameters

SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source IPv6 address or any destination IPv6 address.
host *SRC-IPV6-ADDR*	Specifies a specific source host IPv6 address.
SRC-IPV6-ADDR/PREFIX-LENGTH	Specifies a source IPv6 network.
host *DST-IPV6-ADDR*	Specifies a specific destination host IPv6 address.
DST-IPV6-ADDR/PREFIX-LENGTH	Specifies a destination IPv6 network.
tcp, udp, icmp, esp, pcp ,sctp	Specifies the Layer 4 protocol type.
dscp *VALUE*	(Optional) Specifies the matching traffic class value in IPv6 header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
traffic-class *VALUE*	(Optional) Specifies the matching traffic class value in the IPv6 header. The range is from 0 to 255.
MASK	(Optional) Specifies the traffic class mask (0x0-0xff). If not specified, 0xff is used.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if fall within the range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255.
MASK	(Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number of the message type is from 0 to 255.

ICMP-CODE	(Optional)Specifies the ICMP message code. The valid number of the code type is from 0 to 255.
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, echo-request, erroneous_header, hop-limit, multicast-listener-query, multicast-listener-done, multicast-listener-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
flow-label *FLOW-LABEL*	(Optional) Specifies the flow label value, within the range of 0 to 1048575.
MASK	(Optional) Specifies the flow label mask (0x0-0xfffff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. If not specified, 0xfffff is used.
fragments	(Optional) Specifies the packet fragment's filtering.
time-range *PROFILE-NAME*	(Optional) Specifies the name of time period profile associated with the access list delineating its activation period.

Default

None.

Command Mode

IPv6 Access-list Configuration Mode.

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the command access-list sequence to change the start sequence number and increment number for the specified access list. After the command is applied, the new rule without specified sequence number will be assigned sequence based new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will create extra effort to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access-list. If you enter a sequence number that is already present, an error message will be shown.

The VLAN range and the TCP/UDP port range can only be assigned to an ingress interface.

Example

This example shows how to create four entries for an IPv6 extended access list named “ipv6-control”. These entries are: permit TCP packets destined to network ff02::0:2/16, permit TCP packets destined to host ff02::1:2, permit all TCP packets go to port 80 and permit all ICMP packets.

```
Switch# configure terminal
Switch(config)# ipv6 access-list extended ipv6-control
Switch(config-ipv6-ext-acl)# permit tcp any ff02::0:2/16
Switch(config-ipv6-ext-acl)# permit tcp any host ff02::1:2
Switch(config-ipv6-ext-acl)# permit tcp any any eq 80
Switch(config-ipv6-ext-acl)# permit icmp any any
Switch(config-ipv6-ext-acl)#
```

This example shows how to create two entries for an IPv6 standard access-list named “ipv6-std-control”. These entries are: permit IP packets destined to network ff02::0:2/16, and permit IP packets destined to host ff02::1:2.

```
Switch# configure terminal
Switch(config)# ipv6 access-list ipv6-std-control
Switch(config-ipv6-acl)# permit any ff02::0:2/16
Switch(config-ipv6-acl)# permit any host ff02::1:2
Switch(config-ipv6-acl)#
```

4-13 permit | deny (mac access-list)

This command is used to define the rule for packets that will be permitted or denied. Use the **no** form of this command to remove an entry

[*SEQUENCE-NUMBER***] {permit | deny } {any | host** *SRC-MAC-ADDR* **|** *SRC-MAC-ADDR SRC-MAC-WILDCARD***} {any | host** *DST-MAC-ADDR* **|** *DST-MAC-ADDR DST-MAC-WILDCARD***} [ethernet-type** *TYPE MASK* **[cos** *VALUE* **[***MASK***]] [{vlan** *VLAN-ID* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***}] [time-range** *PROFILE-NAME***]**

no *SEQUENCE-NUMBER*

Parameters

SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source MAC address or any destination MAC address.
host *SRC-MAC-ADDR*	Specifies a specific source host MAC address.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Specifies a group of source MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-MAC-ADDR*	Specifies a specific destination host MAC address.
DST-MAC-ADDR DST-MAC-WILDCARD	Specifies a group of destination MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
ethernet-type *TYPE MASK*	(Optional) Specifies that the Ethernet type which is a hexadecimal number from 0 to FFFF or the name of an Ethernet type which can be one of the following: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp., arp.
cos *VALUE*	(Optional) Specifies the priority value of 0 to 7.
MASK	(Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked. If not specified, 0x7 is used.

vlan *VLAN-ID*	(Optional) Specifies the VLAN-ID.
MASK	(Optional) Specifies the outer VLAN ID mask (0x0-0x0fff). If not specified, 0x0fff is used.
vlan-range *MIN-VID MAX-VID*	(Optional) Specifies the VLAN range. Enter the minimum and maximum VLAN ID in the range here.
time-range *PROFILE-NAME*	(Optional) Specifies the name of time period profile associated with the access list delineating its activation period.

Default

None.

Command Mode

MAC Access-list Configuration Mode.

Usage Guideline

If a rule entry is created without a sequence number, a sequence number will be automatically assigned. If it is the first entry, the sequence number 10 is assigned. A subsequent rule entry will be assigned a sequence number that is 10 greater than the largest sequence number in that access list and is placed at the end of the list.

The user can use the command access-list sequence to change the start sequence number and increment number for the specified access list. After the command is applied, the new rule without specified sequence number will be assigned sequence based new sequence setting of the specified access list.

When you manually assign the sequence number, it is better to have a reserved interval for future lower sequence number entries. Otherwise, it will create extra effort to insert an entry with a lower sequence number.

The sequence number must be unique in the domain of an access-list. If you enter a sequence number that is already present, an error message will be displayed.

The VLAN range can only be assigned to an ingress interface.

Multiple entries can be added to the list, and you can use permit for one entry and use deny for the other entry. Different permit and deny commands can match different fields available for setting.

Example

This example shows how to configure MAC access entries in the profile daily-profile to allow two sets of source MAC addresses.

```
Switch# configure terminal
Switch(config)# mac access-list extended daily-profile
Switch(config-mac-ext-acl)# permit 00:80:33:00:00:00  00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)# permit 00:f4:57:00:00:00 00:00:00:ff:ff:ff any
Switch(config-mac-ext-acl)#
```

4-14 show access-group

This command is used to display access group information for interface(s).

show access-group [interface *INTERFACE-ID***]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all interfaces that have access list configured will be displayed.

Example

This example shows how to display all interfaces that have access lists configured.

```
Switch# show access-group

eth1/0/1:
  Inbound mac access-list : simple-mac-acl(ID: 7998)
  Inbound ip access-list  : simple-ip-acl(ID: 1998)

Switch#
```

4-15 show access-list

This command is used to display the access list configuration information.

show access-list [ip [*NAME* **|** *NUMBER***] | mac [***NAME* **|** *NUMBER***] | ipv6 [***NAME* **|** *NUMBER***] | arp [***NAME***]]**

Parameters

ip	(Optional) Specifies to display a listing of all IP access lists.
mac	(Optional) Specifies to display a listing of all MAC access lists.
ipv6	(Optional) Specifies to display a listing of all IPv6 access lists.
arp	(Optional) Specifies to display the ARP access list.
NAME	(Optional) Specifies to the name of the access list to be displayed.
NUMBER	(Optional) Specifies to the ID of the access list to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to access list information. If no parameter is specified, a listing of all configured access lists is displayed. If the type of access list is specified, detailed information of the access list will be displayed. If the user enables the ACL hardware counter for an access list, the counter will be displayed based on each access list entry.

Example

This example shows how to display all access lists.

```
Switch# show access-list

Access-List-Name                                Type
----------------------------------------   ---------------
Strict-Control(ID: 3999)                   ip ext-acl
daily-profile(ID: 7999)                    mac ext-acl
ip6-control(ID: 14999)                     ipv6 ext-acl

Total Entries: 3


Switch#
```

This example shows how to display the IP access list called “Strict-Control”.

```
Switch# show access-list ip Strict-Control

Extended IP access list Strict-Control(ID: 3999)
    10 permit any 10.20.0.0 0.0.255.255
    20 permit any host 10.100.1.2

Switch#
```

This example shows how to display the content for the access list if its hardware counter is enabled.

```
Switch# show access-list ip simple-ip-acl

Extended IP access simple-ip-acl(ID:3994)
    10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 6410 packets  Egr: 5201 packets)
    20 permit tcp any host 10.100.1.2   (Ing: 3232 packets  Egr: 0 packets)
    30 permit icmp any any   (Ing: 8758 packets  Egr: 4214 packets)

    Counter enable on following port(s):
 Ingress port(s): eth1/0/5-1/0/8
 Egress port(s): eth1/0/3

Switch#
```

5. Access Management Commands

5-1 access-class

This command is used to specify an access list to restrict the access via a line. Use the **no** form of this command to remove the specified access list check.

access-class *IP-ACL*

no access-class *IP-ACL*

Parameters

IP-ACL	Specifies a standard IP access list. The source address field of the permit or deny entry define the valid or invalid host.

Default

None.

Command Mode

Line Configuration Mode.

Usage Guideline

Use this command to specify access lists to restrict the access via a line. At most two access lists can be applied to a line. If two access lists are already applied, an attempt to apply a new access list will be rejected until an applied access list is removed by the **no** form of this command.

Example

This example shows how to create a standard IP access list and specify as the access list to restrict access via Telnet. Only the host 226.1.1.1 is allowed to access the server.

```
Switch#configure terminal
Switch(config)# ip access-list vty-filter
Switch(config-ip-acl)# permit 226.1.1.1 0.0.0.0
Switch(config-ip-acl)# exit
Switch(config)# line telnet
Switch(config-line)# access-class vty-filter
Switch(config-line)#
```

5-2 do

This command is used to execute commands orginally in the EXEC Mode in the Global Configuration Mode.

do *COMMAND*

Parameters

None.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to execute commands orginally in the EXEC Mode, such as **show**, **clear**, or **debug**, while configuring the Switch. After the command is executed, the system will return to the configuration mode you were using.

NOTE: The question mark (?) and the Tab key are available for the do command.

Example

This example shows how to use the question mark (?) with this command.

```
Switch# configure terminal
Switch(config)#do show running-config ?
  all         All configurations including commands corresponding to default
              parameters
  effective   The configurations which affect the behavior of the device
  interface   Select an interface
  Vlan        VLAN configuration
  |           Output modifiers
  <cr>

Switch(config)#do show running-config
```

This example shows how to excute the **show ip interface** command in the Global Configuration Mode.

```
Switch#configure terminal
Switch(config)#do show ip interface

Interface vlan1 is enabled, Link status is down
  IP Address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.

Total Entries: 1

Switch(config)#
```

5-3 ip http server

This command is used to enable the HTTP server. Use the **no** form of this command to disable the HTTP server function.

ip http server

no ip http server

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the HTTP server function. The HTTPs access interface is separately controlled by SSL commands.

Example

This example shows how to enable the HTTP server.

```
Switch#configure terminal
Switch(config)#ip http server
Switch(config)#
```

5-4 ip http secure-server

This command is used to enable the HTTPS server. Use the **ip http secure-server ssl-service-policy** command to specify which SSL service policy is used for HTTPS. Use the **no** form of this command to disable the HTTPS server function.

ip http secure-server [ssl-service-policy *POLICY-NAME***]**

no ip http secure-server

Parameters

ssl-service-policy *POLICY-NAME*	(Optional) Specifies the SSL service policy name. Use this **ssl-service-policy** parameter only if you have already declared an SSL service policy using the **ssl-service-policy** command.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the HTTPS server function and use the specified SSL service policy for HTTPS. If no parameter is specified, a built-in local certificate will be used for HTTPS.

Example

This example shows how to enable the HTTPS server function and use the service policy called “sp1” for HTTPS.

```
Switch# configure terminal
Switch(config)# ip http secure-server ssl-service-policy sp1
Switch(config)#
```

5-5 ip {http | https} access-class

This command is used to specify an access list to restrict the access to the HTTP or HTTPs server. Use the **no** form of this command to remove the access list check.

ip {http | https} access-class *IP-ACL*

no ip {http | https} access-class *IP-ACL*

Parameters

IP-ACL	Specifies a standard IP access list. The source address field of the entry defines the valid or invalid host.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify an access list to restrict the access to the HTTP or HTTPs server. If the specified access list does not exist, the command does not take effect and no access list is checked for the user's access to HTTP or HTTPs.

Example

This example shows how to create a standard IP access list and specify as the access list to access the HTTP server. Only the host 226.1.1.1 is allowed to access the server.

```
Switch# configure terminal
Switch(config)# ip access-list http-filter
Switch(config-ip-acl)# permit 226.1.1.1 255.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# ip http access-class http-filter
Switch(config)#
```

5-6 ip http service-port

This command is used to specify the HTTP service port. Use the **no** form of this command to revert to the default setting.

ip http service-port *TCP-PORT*

no ip http service-port

Parameters

TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The "well-known" TCP port for the HTTP protocol is 80.

Default

By default, this port number is 80.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the TCP port number for the HTTP server.

Example

This example shows how to configure the HTTP TCP port number to 8080.

```
Switch# configure terminal
Switch(config)# ip http service-port 8080
Switch(config)#
```

5-7 ip http timeout-policy idle

This command is used to set idle timeout of a http server connection in seconds. Use the **no** form of this command to set the idle timeout to default value.

ip http timeout-policy idle *INT*

no ip http timeout-policy idle

Parameters

INT	Specifies the idle timeout value. This value is between 60 and 36000.

Default

By default, this value is 180 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the idle timeout value of a http server connection in seconds.

Example

This example shows how to configure the idle timeout value to 100 seconds.

```
Switch# configure terminal
Switch(config)#ip http timeout-policy idle 100
Switch(config)#
```

5-8 ip telnet server

This command is used to enable a Telnet server. Use the **no** form of this command to disable the Telnet server function.

ip telnet server

no ip telnet server

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the Telnet server. The SSH access interface is separately controlled by SSH commands.

Example

This example shows how to enable the Telnet server.

```
Switch# configure terminal
Switch(config)# ip telnet server
Switch(config)#
```

5-9 ip telnet service-port

This command is used to specify the service port for Telnet. Use the **no** form of this command to revert to the default setting.

ip telnet service-port *TCP-PORT*

no ip telnet service-port

Parameters

TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the TELNET protocol is 23.

Default

By default, this port number is 23.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the TCP port number for Telnet access.

Example

This example shows how to change the Telnet service port number to 3000.

```
Switch# configure terminal
Switch(config)# ip telnet service-port 3000
Switch(config)#
```

5-10 line

This command is used to identify a line type for configuration and enter the Line Configuration Mode.

line {console | telnet | ssh}

Parameters

console	Specifies the local console terminal line.
telnet	Specifies the Telnet terminal line.
ssh	Specifies the SSH terminal line.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the Line Configuration Mode.

Example

This example shows how to enter the Line Configuration Mode for the SSH terminal line and configures its access class as ”vty-filter”.

```
Switch# configure terminal
Switch(config)# line ssh
Switch(config-line)# access-class vty-filter
Switch(config-line)#
```

5-11 show terminal

This command is used to display information about the terminal configuration parameter settings for the current terminal line.

show terminal

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the terminal configuration parameters for the current terminal line.

Example

This example shows how to display information about the terminal configuration parameter settings for the current terminal line.

```
Switch#show terminal
Terminal Settings:
 Length: 24 lines
 width: 80 columns
 Default Length: 24 lines
 Default Width: 80 columns
 Baud Rate: 115200 bps

Switch#
```

5-12 show ip telnet server

This command is used to display information about the Telnet server status.

show ip telnet server

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the Telnet server status.

Example

This example shows how to display information about the Telnet server status.

```
Switch#show ip telnet server

Server State: Enabled


Switch#
```

5-13 show ip http server

This command is used to display information about the HTTP server status.

show ip http server

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the HTTP server status.

Example

This example shows how to display information about the HTTP server status.

```
Switch#show ip http server

ip http server state :  Enabled
Switch#
```

5-14 show ip http secure-server

This command is used to display information about the SSL status.

show ip http secure-server

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the SSL status.

Example

This example shows how to display information about the SSL status.

```
Switch#show ip http secure-server

ip http secure-server state :  Disabled
Switch#
```

5-15 show users

This command is used to display information about the active lines on the Switch.

show users

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the active lines on the Switch.

Example

This example shows how to display all session information.

```
Switch#show users
ID   Type      User-Name       Login-Time          IP address
------------------------------------------------------------------------
0    * console admin           25M58S

Total Entries: 1

Switch#
```

5-16 terminal length

This command is used to configure the number of lines displayed on the screen. The **terminal length** command will only affect the current session. The **terminal length default** command will set the default value but it does not affect the current session. The newly created, saved session terminal length will use the default value. Use the **no** form of this command to revert to the default setting.

terminal length *NUMBER*

no terminal length

terminal length default *NUMBER*

no terminal length default

Parameters

NUMBER	Specifies the number of lines to display on the screen. This value must be between 0 and 512.When the terminal length is 0, the display will not stop until it reaches the end of the display.

Default

By default, this value is 24.

Command Mode

EXEC Mode (for the **terminal length** command).

Global Configuration Mode (for the **terminal length default** command).

Usage Guideline

When the terminal length is 0, the display will not stop until it reaches the end of the display.

If the terminal length is specified to a value other than 0, for example 50, the display will stop after every 50 lines. The terminal length is used to set the number of lines displayed on the current terminal screen. This command also applies to Telnet and SSH sessions.

Output from a single command that overflows a single display screen is followed by the **--More--** prompt. At the **--More--** prompt, press CTRL+C, q, Q, or ESC to interrupt the output and return to the prompt. Press the Spacebar to display an additional screen of output, or press Return to display one more line of output. Setting the screen length to 0 turns off the scrolling feature and causes the entire output to display at once. Unless the **default** keyword is used, a change to the terminal length value applies only to the current session. When using the **no** form of this command, the number of lines in the terminal display screen is reset to 24.

The **terminal length default** command is available in the Global Configuration Mode. The command setting does not affect the current existing terminal sessions but affects the new terminal sessions that are activated later. Only the default terminal length value can be saved.

Example

This example shows how to change the lines to be displayed on a screen to 60.

```
Switch# terminal length 60
Switch#
```

5-17 terminal speed

This command is used to setup the terminal speed. Use the **no** form of this command to revert to the default setting.

terminal speed *BPS*

no terminal speed

Parameters

BPS	Specifies the console rate in bits per second (bps).

Default

By default, this value is 115200.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the terminal connection speed. Some baud rates available on the devices connected to the port might not be supported on the Switch.

Example

This example shows how to configure the serial port baud rate to 9600 bps.

```
Switch# configure terminal
Switch(config)# terminal speed 9600
Switch(config)#
```

5-18 session-timeout

This command is used to configure the line session timeout value. Use the **no** form of this command to revert to the default setting.

session-timeout *MINUTES*

no session-timeout

Parameters

MINUTES	Specifies the timeout length in minutes. 0 represents never timeout.

Default

By default, this value is 3 minutes.

Command Mode

Line Configuration Mode.

Usage Guideline

This timer specifies the timeout for auto-logout sessions established by the line that is being configured.

Example

This example shows how to configure the console session to never timeout.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# session-timeout 0
Switch(config-line)#
```

5-19 terminal width

This command is used to set the number of character columns on the terminal screen for the current session line. The **terminal width** command will only affect the current session. The **terminal width default** command will set the default value, but it does not affect any current sessions. Use the **no** form of this command to revert to the default setting.

terminal width *NUMBER*

no terminal width

terminal width default *NUMBER*

no terminal width default

Parameters

NUMBER	Specifies the number of characters to display on the screen. Valid values are from 40 to 255.

Default

By default, this value is 80 characters.

Command Mode

EXEC Mode (for the **terminal width** command).

Global Configuration Mode (for the **terminal width default** command).

Usage Guideline

Use the **terminal width** command to change the terminal width value which applies only to the current session. When changing the value in a session, the value applies only to that session. When the **no** form of this command is used, the number of lines in the terminal display screen is reset to the default.

The **terminal width default** command is available in the Global Configuration Mode. The command setting does not affect the current existing terminal sessions but affect the new terminal sessions that are activated later and just the global terminal width value can be saved.

However, for remote CLI session access such as Telnet, the auto-negotiation terminal width result will take precedence over the default setting if the negotiation is successful. Otherwise, the default setting takes effect.

Example

This example shows how to adjust the terminal width for the current session to 120 characters.

```
Switch#terminal width 120
Switch#
```

5-20 username

This command is used to create a user account. Use the **no** form of this command to delete the user account.

username *NAME* **[nopassword | password** *PASSWORD***]**

no username [*NAME***]**

Parameters

NAME	Specifies the user name with a maximum of 32 characters.
nopassword	(Optional) Specifies that there will be no password associated with this account.
password	(Optional) Specifies the password for the user.
PASSWORD	(Optional) Specifies the password string.

Default

By default, the user name is *admin*, and password is *admin*.

Command Mode

Global Configuration Mode.

Usage Guideline

This command creates user accounts. When the user logs in, the user will be in the EXEC Mode.

If the no username command is used without the user name specified, all users are removed.

When the user account is empty, the user will be directly in the EXEC Mode.

Example

This example shows how to create an administrative username, called “admin”, and a password, called “mypassword”.

```
Switch# configure terminal
Switch(config)# username admin password mypassword
Switch(config)#
```

This example shows how to remove the user account with the username “admin”.

```
Switch# configure terminal
Switch(config)# no username admin
Switch(config)#
```

5-21 clear line

This command is used to disconnect a connection session.

clear line *LINE-ID*

Parameters

LINE-ID	Specifies the line ID of the connection session that will be disconnected.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

Use this command to disconnect an active session on the Switch. The line ID is assigned by line when the connection session was created. Use the **show users** command to view active sessions.

This command can only disconnect SSH and Telnet sessions.

Example

This example shows how to disconnect the line session 1.

```
Switch#clear line 1
Switch#
```

6. ARP Spoofing Prevention Commands

6-1 ip arp spoofing-prevention

This command is used to configure an ARP Spoofing Prevention (ASP) entry of the gateway used for preventing ARP poisoning attacks. Use the **no** form of this command to delete an ARP spoofing prevention entry.

ip arp spoofing-prevention *GATEWAY-IP GATEWAY-MAC* **interface** *INTERFACE-ID* **[, | -]**

no ip arp spoofing-prevention *GATEWAY-IP* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

GATEWAY-IP	Specifies the IP address of the gateway.
GATEWAY-MAC	Specifies the MAC address of the gateway. The MAC address setting will replace the last configuration for the same gateway IP address.
interface *INTERFACE-ID*	Specifies the interface that will be activated or removed from active interface list (in the **no** form of this command). An ARP entry won't be checked, if the receiving port is not included in the specified interface list.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, no entries exist.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to configure the ARP spoofing prevention (ASP) entry to prevent spoofing of the MAC address of the protected gateway. When an entry is created, ARP packets whose sender IP address matches the gateway IP address, of an entry, but its sender MAC address field does not match the gateway MAC address, of the entry, will be dropped by the system. The ASP will bypass the ARP packets whose sender IP address doesn't match the configured gateway IP address.

If an ARP address matches a configured gateway's IP address, MAC address, and port list, then bypass the Dynamic ARP Inspection (DAI) check no matter if the receiving port is ARP 'trusted' or 'untrusted'.

Example

This example shows how to configure an ARP spoofing prevention entry with an IP address of 10.254.254.251 and MAC address of 00-00-00-11-11-11 and activate the entry on port 10.

```
Switch# configure terminal
Switch(config)# ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface
eth1/0/10
Switch(config)# ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface port-
channel 3
Switch(config)#
```

6-2 show ip arp spoofing-prevention

This command is used to display the configuration of ARP spoofing prevention.

show ip arp spoofing-prevention

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display all ARP spoofing prevention entries.

Example

This example shows how to display all ARP spoofing prevention entries.

```
Switch# show ip arp spoofing-prevention

IP              MAC               Interfaces
--------------- ----------------- --------------------------
10.254.254.251  00-00-00-11-11-11 eth1/0/10

Total Entries: 1

Switch#
```

Display Parameters

IP	The IP address of the gateway.
MAC	The MAC address of the gateway.
Interfaces	The interfaces on which the ARP spoofing prevention is active.

7. Asymmetric VLAN Commands

7-1 asymmetric-vlan

This command is used to enable the asymmetric VLAN function. Use the **no** form of this command to disable the asymmetric VLAN function.

asymmetric-vlan

no asymmetric-vlan

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the asymmetric VLAN function.

Example

This example shows how to enable asymmetric VLAN.

```
Switch# configure terminal
Switch(config)# asymmetric-vlan
```

This example shows how to disable asymmetric VLAN.

```
Switch# configure terminal
Switch(config)# no asymmetric-vlan
```

8. Authentication, Authorization, and Accounting (AAA) Commands

8-1 aaa authentication dot1x

This command is used to configure the default method list used for 802.1X authentication. Use the **no** form of this command to remove the default method list.

aaa authentication dot1x default *METHOD1* **[***METHOD2***...]**

no aaa authentication dot1x default

Parameters

METHOD1 **[***METHOD2***...]**	Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. • **local -** Specifies to use the local database for authentication. • **group radius -** Specifies to use the servers defined by the RADIUS server host command. • **group** *GROUP-NAME* **-** Specifies to use the server groups defined by the AAA group server. • **none -** Normally, the method is listed as the last method. The user will pass the authentication if it is not denied by previous method authentication.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the default authentication method list for 802.1X authentication. Initially, the default method list is not configured. The authentication of 802.1X requests will be performed based on the local database.

Example

This example shows how to set the default methods list for authenticating dot1X users.

```
Switch# configure terminal
Switch(config)# aaa authentication dot1x default group radius
Switch(config)#
```

8-2 aaa group server radius

This command is used to enter the RADIUS Group Server Configuration Mode to associate server hosts with the group. Use the **no** form of this command to remove a RADIUS server group.

aaa group server radius *GROUP-NAME*

no aaa group server radius *GROUP-NAME*

Parameters

GROUP-NAME	Specifies the name of the server group. This name can be up to 32 characters long. The syntax is a general string and does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to define a RADIUS server group. The defined server group can be specified as the method list for authentication via the **aaa authentication** command. Also use this command to enter the RADIUS Group Server Configuration Mode. Use the **server** command to associate the RADIUS server hosts with the RADIUS server group.

Example

This example shows how to create a RADIUS server group with two entries. The second host entry acts as backup to the first entry.

```
Switch# configure terminal
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)# server 172.19.10.100
Switch(config-sg-radius)# server 172.19.11.20
Switch(config-sg-radius)# exit
Switch(config)#
```

8-3 aaa new-model

This command is used to enable AAA for the authentication function. Use the **no** form of this command to disable the AAA function.

aaa new-model

no aaa new-model

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable AAA before the authentication via the AAA method lists takes effect. If AAA is disabled, the login user will be authenticated via the local user account table created by the **username** command.

Example

This example shows how to enable the AAA function.

```
Switch# configure terminal
Switch(config)# aaa new-model
Switch(config)#
```

8-4 clear aaa counters servers

This command is used to clear the authentication server statistic counters.

clear aaa counters servers {all | radius {*IP-ADDRESS* **|** *IPV6-ADDRESS* **| all} | sg** *NAME***}**

Parameters

all	Specifies to clear server counter information related to all server hosts.
radius *IP-ADDRESS*	Specifies to clear server counter information related to a RADIUS IPv4 host.
radius *IPV6-ADDRESS*	Specifies to clear server counter information related to a RADIUS IPv6 host.
radius all	Specifies to clear server counter information related to all RADIUS hosts.
sg *NAME*	Specifies to clear server counter information related to all hosts in a server group.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the statistics counter related to AAA servers.

Example

This example shows how to clear AAA server counters.

```
Switch#clear aaa counters servers all
Switch#
```

This example shows how to clear AAA server counters information for all hosts in the server group “server-farm”.

```
Switch#clear aaa counters servers sg server-farm
Switch#
```

8-5 radius-server deadtime

This command is used to specify the default duration of the time to skip the unresponsive server. Use the **no** form of this command to revert to the default setting.

radius-server deadtime *MINUTES*

no radius-server deadtime

Parameters

MINUTES	Specifies the dead time. The valid range is 0 to 1440 (24 hours). When the setting is 0, the unresponsive server will not be marked as dead.

Default

By default, this value is 0.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to improve the authentication processing time by setting the dead time to skip the unresponsive server host entries.

When the system performs authentication with the authentication server, it attempts one server at a time. If the attempted server does not respond, the system will attempt the next server. When the system finds a server does not respond, it will mark the server as down, start a dead time timer, and skip them in authentication of the following requests until expiration of the dead time.

Example

This example shows how to set the dead time to ten minutes.

```
Switch# configure terminal
Switch(config)# radius-server deadtime 10
Switch(config)#
```

8-6 radius-server host

This command is used to create a RADIUS server host. Use the **no** form of this command to delete a server host.

radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [auth-port** *PORT***] [timeout** *SECONDS***] [retransmit** *COUNT***] key** *KEY-STRING*

no radius-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IP address of the RADIUS server.
IPV6-ADDRESS	Specifies the IPv6 address of the RADIUS server.
auth-port *PORT*	(Optional) Specifies the UDP destination port number for sending authentication packets. The range is 0 to 65535. Set the port number to zero if the server host is not for authentication purposes. The default value is 1812.
timeout *SECONDS*	(Optional) Specifies the server time-out value. The range of timeout is between 1 and 255 seconds. If not specified, the default value is 5 seconds.
retransmit *COUNT*	(Optional) Specifies the retransmit times of requests to the server when no response is received. The value is from 0 to 20. Use 0 to disable the retransmission. If not specified, the default value is 2.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can between 1 and 254 clear text characters.

Default

By default, no server is configured.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create RADIUS server hosts before it can be associated with the RADIUS server group using the server command.

Example

This example shows how to create two RADIUS server hosts with the different IP address.

```
Switch# configure terminal
Switch(config)# radius-server host 172.19.10.100 auth-port 1500 timeout 8 retransmit 3 key
ABCDE
Switch(config)# radius-server host 172.19.10.101 auth-port 1600 timeout 3 retransmit 1 key
ABCDE
Switch(config)#
```

8-7 server (RADIUS)

This command is used to associate a RADIUS server host with a RADIUS server group. Use the **no** form of this command to remove a server host from the server group.

server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

no server {*IP-ADDRESS***|** *IPV6-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the authentication server.
IPV6-ADDRESS	Specifies the IPv6 address of the authentication server.

Default

By default, no server is configured.

Command Mode

RADIUS Group Server Configuration Mode.

Usage Guideline

Use this command to associate the RADIUS server hosts with the RADIUS server group. The defined server group can be specified as the method list for authentication via the **aaa authentication** command. Use the **radius-server host** command to create a server host entry. A host entry is identified by IP Address.

Example

This example shows how to create two RADIUS server hosts with the different IP addresses. A server group is then created with the two server hosts.

```
Switch# configure terminal
Switch(config)# radius-server host 172.19.10.100 auth-port 1500 timeout 8 retransmit 3 key
ABCDE
Switch(config)# radius-server host 172.19.10.101 auth-port 1600 timeout 3 retransmit 1 key
ABCDE
Switch(config)#aaa group server radius group1
Switch(config-sg-radius)# server 172.19.10.100
Switch(config-sg-radius)# server 172.19.10.101
Switch(config-sg-radius)#
```

8-8 show aaa

This command is used to display the AAA global state.

show aaa

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the AAA global state.

Example

This example shows how to display the AAA global state.

```
Switch# show aaa

AAA is enabled.

Switch#
```

8-9 show radius statistics

This command is used to display RADIUS statistics for authentication packets.

show radius statistics

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display statistics counters related to servers.

Example

This example shows how to display the server related statistics counters.

```
Switch#show radius statistics

 RADIUS Server: 172.19.10.100: Auth-Port 1500
 State is Up
                         Auth.
 Round Trip Time:        0
 Access Requests:        0
 Access Accepts:         0
 Access Rejects:         0
 Access Challenges:      0
 Retransmissions:        0
 Malformed Responses:    0
 Bad Authenticators:     0
 Pending Requests:       0
 Timeouts:               0
 Unknown Types:          0
 Packets Dropped:        0

 RADIUS Server: 172.19.10.101: Auth-Port 1600
 State is Up
                         Auth.
 Round Trip Time:        0
 Access Requests:        0
 Access Accepts:         0
 Access Rejects:         0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Display Parameters

Auth.	Statistics for authentication packets.
Round Trip Time	The time interval (in hundredths of a second) between the most recent Response and the Request that matched it from this RADIUS server.
Access Requests	The number of RADIUS Access-Request packets sent to this server. This does not include retransmissions.
Access Accepts	The number of RADIUS Access-Accept packets (valid or invalid) received from this server.
Access Rejects	The number of RADIUS Access-Reject packets (valid or invalid) received from this server.
Access Challenges	The number of RADIUS Access-Challenge packets (valid or invalid) received from this server.

Retransmissions	The number of RADIUS Request packets retransmitted to this RADIUS server. Retransmissions include retries where the Identifier and Acct-Delay have been updated, as well as those in which they remain the same.
Malformed Responses	The number of malformed RADIUS Response packets received from this server. Malformed packets include packets with an invalid length. Bad authenticators or Signature attributes or unknown types are not included as malformed responses.
Bad Authenticators	The number of RADIUS Response packets containing invalid authenticators or Signature attributes received from this server.
Pending Requests	The number of RADIUS Request packets destined for this server that have not yet timed out or received a response. This variable is incremented when a Request is sent and decremented due to receipt of a Response, a timeout, or retransmission.
Timeouts	The number of timeouts to this server. After a timeout the client may retry to the same server, send to a different server, or give up. A retry to the same server is counted as a retransmit as well as a timeout. A send to a different server is counted as a Request as well as a timeout.
Unknown Types	The number of RADIUS packets of unknown type which were received from this server.
Packets Dropped	The number of RADIUS packets of which were received from this server and dropped for some other reason.

9. Basic IPv4 Commands

9-1 arp

This command is used to add a static entry in the Address Resolution Protocol (ARP) cache. Use the **no** form of this command to remove a static entry in the ARP cache.

arp *IP-ADDRESS HARDWARE-ADDRESS*

no arp *IP-ADDRESS HARDWARE-ADDRESS*

Parameters

IP-ADDRESS	Specifies the network layer IP address.
HARDWARE-ADDRESS	Specifies the local data-link Media Access (MAC) address (a 48-bit address).

Default

No static entries are installed in the ARP cache.

Command Mode

Global Configuration Mode.

Usage Guideline

The ARP table keeps the network layer IP address to local data-link MAC address association. The association is kept so that the addresses will not have to be repeatedly resolved. Use this command to add static ARP entries.

Example

This example shows how to add a static ARP entry for a typical Ethernet host.

```
Switch# configure terminal
Switch(config)# arp 10.31.7.19 0800.0900.1834
Switch(config)#
```

9-2 arp timeout

This command is used to set the ARP aging time for the ARP table. Use the **no** form of this command to revert to the default setting.

arp timeout *MINUTES*

no arp timeout

Parameters

MINUTES	Specifies the dynamic entry that will be aged-out if it has no traffic activity within the timeout period. The valid values are from 0 to 65535. If this value is configured as 0, ARP entries will never age out.

Default

The default value is 240 minutes.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to set the ARP aging time for the ARP table.

Example

This example shows how to set the ARP timeout to 60 minutes to allow entries to time out.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# arp timeout 60
Switch(config-if)#
```

9-3 clear arp-cache

This command is used to clear the dynamic ARP entries from the table.

clear arp-cache {all | interface *INTERFACE-ID* **|** *IP-ADDRESS***}**

Parameters

all	Specifies to clear the dynamic ARP cache entries associated with all interfaces.
interface *INTERFACE-ID*	Specifies the interface ID.
IP-ADDRESS	Specifies the IP address of the specified dynamic ARP cache entry that will be cleared.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to delete dynamic entries from the ARP table. The user can select to delete all dynamic entries, specific dynamic entries, or all of the dynamic entries that are associated with a specific interface.

Example

This example shows how to remove all dynamic entries from the ARP cache.

```
Switch# clear arp-cache all
Switch#
```

9-4 ip address

This command is used to set a primary or secondary IPv4 address for an interface, or acquire an IP address on an interface from the DHCP. Use the **no** form of this command to remove the configuration of an IP address or disable DHCP on the interface.

ip address {*IP-ADDRESS SUBNET-MASK* **| dhcp}**

no ip address {*IP-ADDRESS SUBNET-MASK* **| dhcp}**

Parameters

IP-ADDRESS	Specifies the IP address.
SUBNET-MASK	Specifies the subnet mask for the associated IP address.
dhcp	Specifies to acquire an IP address configuration on an interface from the DHCP protocol.

Default

The default IP address for VLAN 1 is 10.90.90.90/8.

Command Mode

Interface Configuration Mode.

Usage Guideline

The IPv4 address of an interface can be either manually assigned by the user or dynamically assigned by the DHCP server. Use the **no ip address** command to delete the configured IP address entry.

NOTE: The Switch supports up to four IPv4 and IPv6 interfaces.

Example

This example shows how to configure 10.108.1.27 as the IP address for VLAN 1.

```
Switch# configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip address 10.108.1.27 255.0.0.0
Switch(config-if)#
```

9-5 show arp

This command is used to display the ARP cache.

show arp [*ARP-TYPE***] [***IP-ADDRESS* **[***MASK***]] [***INTERFACE-ID***] [***HARDWARE-ADDRESS***]**

Parameters

ARP-TYPE	(Optional) Specifies the ARP type. • **dynamic** - Specifies to display only dynamic ARP entries. • **static** - Specifies to display only static ARP entries.
IP-ADDRESS **[***MASK***]**	(Optional) Specifies to display a specific entry or entries that belong to a specific network.
INTERFACE-ID	(Optional) Specifies to display ARP entries that are associated with a specific interface.

HARDWARE-ADDRESS	(Optional) Specifies to display ARP entries whose hardware address equal to this address.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display a specific ARP entry, all ARP entries, dynamic entries, or static entries, or entries associated with an IP interface.

Example

This example shows how to display the ARP cache.

```
Switch# show arp

S - Static Entry

IP Address         Hardware Addr      IP Interface   Age (min)
-----------------  -----------------  -------------  ---------------
S 10.31.7.19       08-00-09-00-18-34  vlan1          forever
  10.90.90.90      00-01-02-03-04-00  vlan1          forever

Total Entries: 2

Switch#
```

9-6 show arp timeout

This command is used to display the aging time of ARP cache.

show arp timeout [interface *INTERFACE-ID***]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the configured ARP aging time.

Example

This example shows how to display the ARP aging time.

```
Switch# show arp timeout

Interface    Timeout (minutes)
------------ -----------------
vlan1        60
------------ -----------------
Total Entries:1

Switch#
```

9-7 show ip interface

This command is used to display the IP interface information.

show ip interface [*INTERFACE-ID***] [brief]**

Parameters

INTERFACE-ID	(Optional) Specifies to display information for the specified IP interface.
brief	(Optional) Specifies to display a summary of the IP interface information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the IP interface information. If no parameter is specified, information for all the interfaces will be displayed.

Example

This example shows how to display the brief information of the IP interface.

```
Switch#show ip interface brief

Interface    IP Address      Link Status
----------  ---------------  -----------
vlan1       10.90.90.90      up

Total Entries: 1

Switch#
```

This example shows how to display the IP interface information for VLAN 1.

```
Switch#show ip interface vlan 1

Interface vlan1 is enabled, Link status is down
  IP address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

10. Basic IPv6 Commands

10-1 clear ipv6 neighbors

This command is used to clear IPv6 neighbor cache dynamic entries.

clear ipv6 neighbors {all | interface *INTERFACE-ID***}**

Parameters

all	Specifies to clear the dynamic neighbor cache entries associated with all interfaces.
interface *INTERFACE-ID*	Specifies to clear dynamic neighbor cache entries associated with the specified interface.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear dynamic neighbor cache entries.

Example

This example shows how to clear IPv6 neighbor cache entries associated with interface VLAN 1.

```
Switch#clear ipv6 neighbors interface vlan1
Switch#
```

10-2 ipv6 address

This command is used to manually configure an IPv6 addresses on the interface. Use the **no** form of this command to delete a manually configured IPv6 address.

ipv6 address {*IPV6-ADDRESSIPREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

no ipv6 address {*IPV6-ADDRESSIPREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

Parameters

IPV6-ADDRESS	Specifies the IPv6 address and the length of prefix for the subnet.
PREFIX-LENGTH	Specifies the length of the prefix. The prefix of the IPv6 address is also a local subnet on the interface.
link-local	Specifies a link-local address to be configured.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

The IPv6 address can directly be specified by the user or configured based on a general prefix. The general prefix can be acquired by the DHCPv6 client. The general prefix does not need to exist before it can be used in the **ipv6 address** command. The IPv6 address will not be configured until the general prefix is acquired. The configured IPv6 address will be removed when the general prefix is timeout or removed. The general prefix IPv6 address is formed by the general prefix in the leading part of bits and the sub-bits excluding the general prefix part in the remaining part of bits.

Each interface can have one IPv6 address assigned. When the IPv6 address is configured on an interface, IPv6 processing is enabled for the interface. The prefix of the configured IPv6 address will automatically be advertised as prefix in the RA messages transmitted on the interface.

Example

This example shows how to configure an IPv6 address.

```
Switch#configure terminal
Switch(config)# interface vlan2
Switch(config-if)# ipv6 address 3ffe:22:33:44::55/64
```

This example shows how to remove an IPv6 address.

```
Switch#configure terminal
Switch(config)# interface vlan2
Switch(config-if)# no ipv6 address 3ffe:22:3:44::55/64
```

10-3 ipv6 address eui-64

This command is used to configure an IPv6 address on the interface using the EUI-64 interface ID. Use the **no** form of this command to delete an IPv6 address formed by the EUI-64 interface ID.

ipv6 address *IPV6-PREFIXIPREFIX-LENGTH* **eui-64**

no ipv6 address *IPV6-PREFIXIPREFIX-LENGTH* **eui-64**

Parameters

IPV6-PREFIX	Specifies the IPv6 prefix part for the configured IPv6 address.
PREFIX-LENGTH	Specifies the length of the prefix. The prefix of the IPv6 address is also a local subnet on the interface. The prefix length must be smaller than 64.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

If the command is configured on an IPv6 ISTAP tunnel, the last 32 bits of the interface ID are constructed using the source IPv4 address of the tunnel.

Example

This example shows how to add an IPv6 address incidence.

```
Switch#configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address 3ffe:501:ffff:0::/64 eui-64
Switch(config-if)#
```

10-4 ipv6 address dhcp

This command is used to configure an interface using DHCPv6 to get an IPv6 address. Use the **no** form of this command to disable the using of DHCPv6 to get an IPv6 address.

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Parameters

rapid-commit	(Optional) Specifies to proceed with two-message exchange for address delegation. The rapid-commit option will be filled in the Solicit message to request two messages handshake.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure the interface to obtain IPv6 network configuration settings from a DHCPv6 server.

The standard four-message exchange between the DR and the RR includes four messages: SOLICIT, ADVERTISE, REQUEST, and REPLY. When the **rapid-commit** parameter is specified, the RR will notify the DR in the SOLICIT message that it can skip receiving the ADVERTISE message and sending REQUEST message, and proceed directly with receiving the REPLY message from DR to complete a two-message exchange instead of the standard four-message exchange. The REPLY message contains the network configuration settings.

The **rapid-commit** parameter must be enabled on both the DR and the RR to function properly.

When the **no** command is used, the existing IPv6 network configuration settings which are obtained from the DHCPv6 server will be removed.

Example

This example shows how to configure VLAN 1 to use DHCPv6 to get an IPv6 address.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address dhcp
Switch(config-if)#
```

10-5 ipv6 address autoconfig

This command is used to enable the automatic configuration of the IPv6 address using the stateless auto-configuration. Use the **no** form of this command to delete an IPv6 address formed by auto-configuration.

ipv6 address autoconfig [default]

no ipv6 address autoconfig

Parameters

default	(Optional) Specifies that if the default router is selected on this interface, this parameter causes a default route to be installed using that default router. This can be specified only on one interface.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command only available for the VLAN IPv6 interface.

When enabling automatic configuration, the interface enables IPv6 processing and the router advertisement containing an assigned global address prefix will be received on this interface from an IPv6 router. Then the resulting address that is a combination of the prefix and the interface identifier will be assigned to the interface. When this option is disabled, the obtained global unicast address will be removed from the interface.

If the **default** parameter is specified, it will accord the received router advertisement to insert a default route to the IPv6 routing table. The type of this default route is SLAAC. It has higher route preference than the dynamic default route which is learnt from RIPng, OSPFv3, and BGP+, but has lower route preference than the static default route.

Example

This example shows how to configure the IPv6 stateless address auto-configuration.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 address autoconfig
Switch(config-if)#
```

10-6 ipv6 enable

This command is used to enable IPv6 processing on interfaces that have no IPv6 address explicitly configured. Use the **no** form of this command to disable IPv6 processing on interfaces that have no IPv6 address explicitly configured.

ipv6 enable

no ipv6 enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

When the IPv6 address is explicitly configured on the interface, the IPv6 link-local address is automatically generated and the IPv6 processing is started. When the interface has no IPv6 address explicitly configured, the IPv6 link-local address is not generated and the IPv6 processing is not started. Use the **ipv6 enable** command to auto-generate the IPv6 link-local address and start the IPv6 processing on the interface.

Example

This example shows how to enable IPv6 on interface VLAN 1, which has no IPv6 address explicitly configured.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 enable
Switch(config-if)#
```

10-7 ipv6 hop-limit

This command is used to configure the IPv6 hop limit on the Switch. Use the **no** form of this command to revert to the default setting.

ipv6 hop-limit *VALUE*

no ipv6 hop-limit

Parameters

VALUE	Specifies the IPv6 hop limit value. To use the default value on this interface, configure this value as 0. The range is from 0 to 255.

Default

By default, this value is 64.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure the hop limit to be advertised in RA messages. The IPv6 packet originated at the system will also use this value as the initial hop limit.

Example

This example shows how to configure the IPv6 hop limit value to 255.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 hop-limit 255
Switch(config-if)#
```

10-8 ipv6 nd managed-config-flag

This command is used to enable the management configure flag in the advertised RA message. Use the **no** command to disable this flag.

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

When the neighboring host receives the RA with an enabled flag, the host should use a stateful configuration protocol to obtain IPv6 addresses.

Example

This example shows how to enable the IPv6 management configure flag in RA advertised on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd managed-config-flag
Switch(config-if)#
```

10-9 ipv6 nd other-config-flag

This command is used to enable the other configure flag in the advertised RA message. Use the **no** command to disable this flag.

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

When this feature is enabled, the router will instruct the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than IPv6 address.

Example

This example shows how to enable the IPv6 other configure flag in RA advertised on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd other-config-flag
Switch(config-if)#
```

10-10 ipv6 nd prefix

This command is used to configure the IPv6 prefix to be advertised in RA messages. Use the **no** command to remove the prefix.

ipv6 nd prefix *IPV6-PREFIXIPREFIX-LENGTH* **[***VALID-LIFETIME PREFERRED-LIFETIME***] [off-link] [no-autoconfig]**

no ipv6 nd prefix *IPV6-PREFIXIPREFIX-LENGTH*

Parameters

IPV6-PREFIX	Enter the IPv6 prefix to be created or advertised in the RA on the interface here.
PREFIX-LENGTH	Enter the IPv6 prefix length to be created or advertised in the RA on the interface here.
VALID-LIFETIME	(Optional) Enter the valid lifetime value here. The range is from 0 to 4294967295 seconds.
PREFERRED-LIFETIME	(Optional) Enter the preferred lifetime value here. The range is from 0 to 4294967295 seconds.
off-link	(Optional) Specifies to disable the on-link flag.
no-autoconfig	(Optional) Specifies to disable the auto-config flag.

Default

The default valid lifetime value is 2592000 seconds (30 days).

The default preferred lifetime value is 604800 seconds (7 days).

By default, the off-link flag and auto-config flag is on.

Command Mode

Interface Configuration Mode.

Usage Guideline

For a prefix, the valid lifetime should be greater than the preferred lifetime. They are meaningful when the prefix has the A bit ON. The received host will do a stateless address configuration based on the prefix. If the lifetime of the prefix has exceeded the preferred lifetime, then the IPv6 address configured based on this prefix will change to the deprecated state. If the lifetime of a prefix has exceeded the valid lifetime, then the IPv6 address configured based on this prefix will be removed.

If the IPv6 address is manually configured on the interface, the corresponding prefix will automatically be advertised. The advertised prefix can be modified but cannot be removed using this command. If the IPv6 address is removed later, the advertising of the corresponding prefix will also be stopped.

Example

This example shows how to configure an IPv6 prefix 3ffe:501:ffff:100::/64 with a valid lifetime of 30000 seconds and a preferred lifetime of 20000 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd prefix 3ffe:501:ffff:100::/64 30000 20000
Switch(config-if)#
```

10-11 ipv6 nd ra interval

This command is used to configure the IPv6 RA interval for an interface. Use the **no** form of this command to revert to the default setting.

ipv6 nd ra interval *MAX-SECS* **[***MIN-SECS***]**

no ipv6 nd ra interval

Parameters

MAX-SECS	Specifies the maximum interval between retransmission of RA messages in seconds. The valid range is from 4 to 1800 seconds.
MIN-SECS	(Optional) Specifies the minimum interval between retransmission of RA messages in seconds. This value must be smaller than 0.75 times the maximum value. The valid range is from 3 to 1350 seconds.

Default

By default, the maximum interval value is 200 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

The following rules apply to the minimum RA interval value if the minimum value is not configured:

- If the maximum RA interval value is equal to or greater than 9 seconds, then the minimum value will be 33% of the maximum value.
- If the maximum RA interval value lesser than 9 seconds, then the minimum value will be the same as the maximum value.

Example

This example shows how to configure IPv6 RA interval value.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd ra interval 1500 1000
Switch(config-if)#
```

10-12 ipv6 nd ra lifetime

This command is used to configure the IPv6 RA lifetime value for an interface. Use the **no** form of this command to revert to the default setting.

ipv6 nd ra lifetime *SECONDS*

no ipv6 nd ra lifetime

Parameters

SECONDS	Specifies the lifetime in seconds of the router as the default router. The valid range is 0-9000.

Default

By default, this value is 1800 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

The lifetime value in RA informs the received host of the lifetime for taking the router as the default router.

Example

This example shows how to configure the lifetime value advertised in the RA to 9000 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd ra lifetime 9000
Switch(config-if)#
```

10-13 ipv6 nd suppress-ra

This command is used to disable the sending of RA messages on the interface. Use the **no** command to enable the sending of RA messages.

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameters

None.

Default

By default, this feature is enabled on a VLAN interface.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for VLAN interface configuration.

Use this command to disable the sending of RA messages on the interface. Use the **no** command to re-enable the sending of RA messages on the interface.

Example

This example shows how to suppress the sending of RA on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd suppress-ra
Switch(config-if)#
```

10-14 ipv6 nd reachable-time

This command is used to configure the reachable time used in the ND protocol. Use the **no** form of this command to revert to the default setting.

ipv6 nd reachable-time *MILLI-SECONDS*

no ipv6 nd reachable-time

Parameters

MILLI-SECONDS	Specifies the IPv6 router advertisement reachable time range in milliseconds. The range is from 0 to 3600000 milliseconds in multiples of 1000 milliseconds.

Default

The default value advertised in RA is 1200000 milliseconds.

The default value used by the router is 1200000 milliseconds (1200 seconds).

Command Mode

Interface Configuration Mode.

Usage Guideline

The configured time is used by the router on the interface and is also advertised in RA message. If the specified time is 0, the router will use 30 seconds on the interface and advertise 0 (unspecified) in RA message. The reachable time is used by the IPv6 node in determining the reachability of the neighboring nodes.

Example

This example shows how to configure the reachable time on VLAN 1 to 3600 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd reachable-time 3600000
Switch(config-if)#
```

10-15 ipv6 nd ns-interval

This command is used to configure the interval between retransmissions of NS messages. Use the **no** form of this command to revert to the default setting.

ipv6 nd ns-interval *MILLI-SECONDS*

no ipv6 nd ns-interval

Parameters

MILLI-SECONDS	Specifies the amount of time between retransmissions of NS message here. The range is from 0 to 3600000 milliseconds in multiples of 1000 milliseconds.

Default

The default value advertised in the RA is 0.

The default value used by the router is 1000 milliseconds (1 second).

Command Mode

Interface Configuration Mode.

Usage Guideline

The configured time is used by the router on the interface and is also advertised in RA message. If the specified time is 0, the router will use 1 second on the interface and advertise 0 (unspecified) in the RA message.

Example

This example shows how to configure the IPv6 NS message retransmission interval to 6 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 nd ns-interval 6000
Switch(config-if)#
```

10-16 ipv6 neighbor

This command is used to create a static ipv6 neighbor entry. Use the **no** form of this command to delete a static IPv6 neighbor entry.

ipv6 neighbor *IPV6-ADDRESS INTERFACE-ID MAC-ADDRESS*

no ipv6 neighbor *IPV6-ADDRESS INTERFACE-ID*

Parameters

IPV6-ADDRESS	Specifies the IPv6 address of the IPv6 neighbor cache entry.
INTERFACE-ID	Specifies the interface of the static IPv6 neighbor cache entry.
MAC-ADDRESS	Specifies the MAC address of the IPv6 neighbor cache entry.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create a static IPv6 neighbor cache entry on an interface. The static entry will be either in the REACHABLE state, if the interface is UP, or in the INCOMPLETE state if the interface is down. The reachable detection process will not be applied to the static entries.

The **clear ipv6 neighbors** command will clear the dynamic neighbor cache entries. Use the **no ipv6 neighbor** command to delete a static neighbor entry.

Example

This example shows how to create a static ipv6 neighbor cache entry.

```
Switch# configure terminal
Switch(config)# ipv6 neighbor fe80::1 vlan1 00-01-80-11-22-99
Switch(config)#
```

10-17 show ipv6 interface

This command is used to display IPv6 interface information.

show ipv6 interface [*INTERFACE-ID***] [brief]**

Parameters

INTERFACE-ID	(Optional) Specifies to display information for the specified IPv6 interface.
brief	(Optional) Specifies to display a summary of the IPv6 interface information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display IPv6 interface related configurations.

Example

This example shows how to display IPv6 interface information.

```
Switch#show ipv6 interface vlan2

vlan2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
      FE80::200:ABFF:FECD:1234
  Global unicast address:
      200::2/64 (Manual)
  RA messages are sent between 66 to 200 seconds
  RA advertised reachable time is 1200000 milliseconds
  RA advertised retransmit interval is 0 milliseconds
  RA advertised life time is 1800 seconds
  RA advertised O flag is OFF, M flag is OFF
  RA advertised prefixes
    200::/64
        valid lifetime is 2592000,  preferred lifetime is 604800

Total Entries: 1

Switch#
```

This example shows how to display brief IPv6 interface information.

```
Switch#show ipv6 interface brief

vlan1 is up, Link status is up
    FE80::201:1FF:FE02:304

vlan2 is up, Link status is down
    FE80::201:1FF:FE02:305
    200::2

vlan3 is up, Link status is down
    FE80::201:1FF:FE02:306

Total Entries: 3

Switch#
```

10-18 show ipv6 neighbors

This command is used to display IPv6 neighbor information.

show ipv6 neighbors [*INTERFACE-ID***] [***IPV6-ADDRESS***]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface to display IPv6 neighbor cache entry.
IPV6-ADDRESS	(Optional) Specifies the IPv6 address to display its IPv6 neighbor cache entry.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the IPv6 neighbor cache entry.

Example

This example shows how to display the IPv6 neighbor cache entry.

```
Switch# show ipv6 neighbors

IPv6 Address                            Link-Layer Addr   Interface Type State
--------------------------------------- ----------------- --------- ---- -----
FE80::200:11FF:FE22:3344                00-00-11-22-33-44 vlan1     D   REACH

Total Entries: 1

Switch#
```

Display Parameters

Type	• **D** - Dynamic learning entry. • **S** - Static neighbor entry.
State	• **INCMP (Incomplete)** - Address resolution is being performed on the entry, but the corresponding neighbor advertisement message has not yet been received. • **REACH (Reachable)** - Corresponding neighbor advertisement message was received and the reachable time (in milliseconds) has not elapsed yet. It indicates that the neighbor was functioning properly. • **STALE** - More than the reachable time (in milliseconds) have elapsed since the last confirmation was received. • **PROBE** - Sending the neighbor solicitation message to confirm the reachability. • **DELAY** - The neighbor is no longer known to be reachable and traffic has recently been sent to the neighbor. Instead of probing the neighbor immediately, delay the sending of probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation.

11. Cable Diagnostics Commands

11-1 test cable-diagnostics

This command is used to start the cable diagnostics to test the status and length of copper cables.

test cable-diagnostics interface *INTERFACE-ID* **[, | -]**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port interface configuration. Cable Diagnostics can help users to detect whether the copper Ethernet port has connectivity problems. Use the test cable-diagnostics command to start the test. The copper port can be in one of the following status:

- **Open** - The cable in the error pair does not have a connection at the specified position.
- **Short** - The cable in the error pair has a short problem at the specified position.
- **Open or Short** - The cable has an open or short problem, but the PHY has no capability to distinguish between them.
- **Crosstalk** - The cable in the error pair has a crosstalk problem at the specified position.
- **Shutdown** - The remote partner is powered off.
- **Unknown** - The test got an unknown status.
- **OK** - The pair or cable has no error.
- **No cable** - The port does not have any cable connection to the remote partner.

Example

This example shows how to start the cable diagnostics to test the status and length of copper cables.

```
Switch#test cable-diagnostics interface eth1/0/1
Switch#
```

11-2 show cable-diagnostics

This command is used to display the test results for the cable diagnostics.

show cable-diagnostics [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface ID.

,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port interface configuration. Use this command to display the test results for the cable diagnostics.

Example

This example shows how to display the test results for the cable diagnostics.

```
Switch#show cable-diagnostics

Port      Type       Link Status   Test Result                Cable Length (M)
--------- ---------- ------------- ------------------------- -----------------
eth1/0/1  10GBASE-T  Link Up       Pair 1 Open      at   2M  -
                                   Pair 2 OK        at   0M
                                   Pair 3 OK        at   0M
                                   Pair 4 Open      at   1M
eth1/0/2  10GBASE-T  Link Down     -                        -
eth1/0/3  10GBASE-T  Link Up       -                        -
eth1/0/4  10GBASE-T  Link Down     -                        -
eth1/0/5  10GBASE-T  Link Down     -                        -
eth1/0/6  10GBASE-T  Link Down     -                        -
eth1/0/7  10GBASE-T  Link Down     -                        -
eth1/0/8  10GBASE-T  Link Down     -                        -
eth1/0/9  10GBASE-T  Link Down     -                        -
eth1/0/10 10GBASE-T  Link Down     -                        -
eth1/0/11 10GBASE-T  Link Down     -                        -
eth1/0/12 10GBASE-T  Link Down     -                        -
eth1/0/13 10GBASE-T  Link Down     -                        -
eth1/0/14 10GBASE-T  Link Down     -                        -
eth1/0/15 10GBASE-T  Link Down     -                        -
eth1/0/16 10GBASE-T  Link Down     -                        -
eth1/0/17 10GBASE-T  Link Down     -                        -
eth1/0/18 10GBASE-T  Link Down     -                        -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

11-3 clear cable-diagnostics

This command is used to clear the test results for the cable diagnostics.

clear cable-diagnostics {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear cable diagnostics results for all interfaces.
interface *INTERFACE-ID*	Specifies the interface ID.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port interface configuration. Use this command to clear the test results for the cable diagnostics. If the test is running on the interface, an error message will be displayed.

Example

This example shows how to clear the test results for the cable diagnostics.

```
Switch# clear cable-diagnostics interface eth1/0/1
Switch#
```

12. Debug Commands

12-1 debug enable

This command is used to enable the debug message output option. Use the **no** form of this command to disable the debug message output option.

debug enable

no debug enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the debug message output option.

Example

This example shows how to enable and then disable the debug message output option.

```
Switch#configure terminal
Switch(config)#debug enable
Switch(config)#no debug enable
Switch(config)#
```

12-2 debug reboot on-error

This command is used to set the Switch to reboot when a fatal error occurs. Use the **no** form of this command to set the Switch not to reboot when a fatal error occurs.

debug reboot on-error

no debug reboot on-error

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the Switch to reboot when a fatal error occurs.

Example

This example shows how to enable the Switch to reboot on fatal errors.

```
Switch#configure terminal
Switch(config)#debug reboot on-error
Switch(config)#
```

12-3 debug copy

This command is used to copy debug information to the destination filename.

debug copy *SOURCE-URL DESTINATION-URL*

debug copy *SOURCE-URL* **{tftp: //***LOCATION**DESTINATION-URL***}**

Parameters

SOURCE-URL	Specifies the source URL for the source file to be copied. It must be one of the following keywords. **error-log:** Specifies to copy the error log information. **tech-support:** Specifies to copy the technical support information. This can only be copied using TFTP.
DESTINATION-URL	Specifies the destination URL.
LOCATION	Specifies the IPv4 or IPv6 address of the TFTP server.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

Use this command to copy debug information to the destination filename. When **tech-support** information is copied and there are more than one Switch unit in the stack, multiple files will be generated containing the Switch unit ID as a suffix in the filename.

Example

This example shows how to copy debug buffer information to a TFTP server (10.90.90.99).

```
Switch# debug copy buffer tftp: //10.90.90.99/abc.txt

Address of remote host [10.90.90.99]?
Destination filename [abc.txt]?
 Accessing tftp://10.90.90.99/abc.txt...
Transmission starts...
Finished network upload(65739) bytes.

Switch#
```

12-4 debug clear error-log

This command is used to clear the error log information.

debug clear error-log

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

Use this command to clear the error log information.

Example

This example shows how to clear the error log information.

```
Switch# debug clear error-log
Switch#
```

12-5 debug show error-log

This command is used to display error log information.

debug show error-log

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

Use this command to display the content of the error log.

Example

This example shows how to display error log information.

```
Switch# debug show error-log

# debug log: 1
# level: fatal
# clock: 10000ms
# time : 2013/03/11 13:00:00
====================== SOFTWARE FATAL ERROR ======================
Invalid mutex handle : 806D6480

Current TASK : bcmARL.0
------------------------- TASK STACKTRACE -----------------------
->802ACE98
->8018C814
->8028FF44
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
->802A5D6C

**************************************************************************
# debug log: 2
# level: fatal
# clock: 10000ms
# time : 2013/03/11 15:00:00
====================== SOFTWARE FATAL ERROR ======================
CLI_UTL_AllocateMemory Fail!

Current TASK : CLI
------------------------- TASK STACKTRACE -----------------------
->802ACE98
->802B4498
->802B4B00
->802BD140
->802BCB08

Total Log : 2

Switch#
```

12-6 debug show tech-support

This command is used to display the information required by technical support personnel.

debug show tech-support

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

Use this command to display technical support information. The technical support information is used to collect the Switch's information needed by the engineers to troubleshoot or analyze a problem.

Example

This example shows how to display technical support information of all the modules.

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#             DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch
#                          Technical Support Information
#
#                            Firmware: Build 1.00.021
#    Copyright(C) 2020  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


********************   Basic System Information   ********************

[SYS 2019-1-1 07:33:49]

Boot Time           : 1 Jan 2019  00:00:00
RTC Time            : 2019/01/01 07:33:49
Bootloader Version  :
Linux Version       : 1.0.5
Runtime Version     : 1.00.021
Hardware Version    : A1
Serial number       : DXS1210102030
MAC Address         : F0-7D-68-12-10-01
MAC Address Number  : 65535

CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

13. DHCP Auto-Configuration Commands

13-1 autoconfig enable

This command is used to enable the auto-configuration function. Use the **no** form of this command to disable the auto-configuration function.

autoconfig enable

no autoconfig enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

When auto-configuration is enabled and the Switch is rebooted, the Switch becomes a DHCP client automatically. The auto-configuration process is as following:

- The Switch will get “configure file path” name and the TFTP server IP address from the DHCP server if the DHCP server has the TFTP server IP address and configuration file name and be configured to deliver this information in the data field of the DHCP reply packet.
- The Switch will then download the configuration file from the TFTP server to configure the system, if the TFTP server is running and have the requested configuration file in its base directory when the request is received from the Switch.

If the Switch is unable to complete the auto-configuration process, the previously saved local configuration file present in switch memory will be loaded.

Example

This example shows how to enable auto-configuration.

```
Switch# configure terminal
Switch(config)# autoconfig enable
Switch(config)#
```

13-2 show autoconfig

This command is used to display the status of auto-configuration.

show autoconfig

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the status of the auto-configuration.

Example

This example shows how to display the status of the auto-configuration.

```
Switch# show autoconfig

Autoconfig State: Disabled

Switch#
```

14. DHCP Auto-Image Commands

14-1 autoimage enable

This command is used to enable the auto-image function. Use the **no** form of this command to disable the auto-image function.

autoimage enable

no autoimage enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

During the start-up time of a switch, this function provides the capability of obtaining the image file form an external TFTP server whose IP address and file name is carried in the DHCP OFFER message received from the DHCP server. The system then uses this image file as the boot-up image file. When the system boots up and the auto-image function is enabled, the Switch becomes a DHCP client automatically.

The DHCP client will be activated to get the network setting from the DHCP server and the DHCP server attaches the TFTP server IP address and image filename to the message. The Switch then catches this information and triggers the TFTP downloading function from this specified TFTP server. At this stage, system will display the download configuration parameters on the console and the layout is the same as using the **download firmware** command.

After the firmware download was completed, the Switch will then reboot immediately.

If both the auto-configuration and auto-image features are enabled at the same time, system will download the image file first and then download the configuration. After this, the Switch will then initiate a save configuration and reboot.

The Switch will always check the acquired firmware. If the version is the same as the current running firmware, the Switch will terminate the auto-image process. The download configuration, however, will still be executed if the auto-configuration feature is also enabled.

This function is similar to the auto-configuration function. The TFTP server IP address is still placed in the DHCP siaddr fields Option 66 or Option 150. If Option 66, Option 150 and the siaddr fields exist in the DHCP response message at the same time, the Option 150 will be resolved first. If the system fails to connect to the TFTP server, the system will resolve the Option 66, and if the system still fails to connect the TFTP server, the siaddr field is the last choice.

When Switch uses Option 66 to get the TFTP server name, it will resolve Option 6 first to get the DNS server IP address. If the Switch fails to connect to the DNS server or Option 6 does not exist in the response message, the Switch will try to connect the DNS server already configured in the system manually.

Because the DHCP option fields are not only used in the auto-image feature but also in the auto-configuration feature, both the image file and the configuration file must be placed on the same TFTP server.

When specifying the image file name, the DHCP Option 125 (RFC 3925) must be used. The Switch needs to check the enterprise-number1 field. If the value is not the D-Link vendor ID (171), the Switch will stop the process. If the Option contains more than one data, only the first data *enterprise-number1* will be used.

Example

This example shows how to how to enable auto-image.

```
Switch#configure terminal
Switch(config)#autoimage enable
Switch(config)#
```

14-2 autoimage timeout

This command is used to specify the length of timeout in second for getting the image file through the network.

autoimage timeout *SECONDS*

Parameters

SECONDS	Specifies the length of timeout in second. The value is form 1 to 65535.

Default

By default, the value is 50 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the length of timeout in second for getting the image file through the network.

Example

This example shows how to configure the timeout value to 60.

```
Switch#configure terminal
Switch(config)#autoimage timeout 60
Switch(config)#
```

14-3 show autoimage

This command is used to display the status of auto-image.

show autoimage

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is used to display the status of the auto- image.

Example

This example shows how to display the status of the auto- image.

```
Switch#show autoimage

Autoimage State: Disabled
Timeout        : 60

Switch#
```

15. DHCP Client Commands

15-1 ip dhcp client class-id

This command is used to specify the vendor class identifier used as the value of Option 60 for the DHCP discover message. Use the **no** form of this command to revert to the default setting.

ip dhcp client class-id {*MULTI-WORD* **| hex** *HEX-STRING***}**

no ip dhcp client class-id

Parameters

MULTI-WORD	Specifies the vendor class identifier in the string form. The maximum length of the string is 32. Space characters are allowed in the string.
hex *HEX-STRING*	Specifies a vendor class identifier in the hexadecimal form. The maximum length of the string is 64.

Default

The device type will be used as the class ID.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to specify a vendor class identifier (Option 60) to be sent with the DHCP discover message. This specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. The vendor class identifier specifies the type of device that is requesting an IP address.

Example

This example shows how to specify the vendor class identifier as VOIP Device for VLAN 100 to be sent with the DHCP discover message.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip address dhcp
Switch(config-if)# ip dhcp client class-id VOIP Device
Switch(config-if)#
```

15-2 ip dhcp client client-id

This command is used to specify the VLAN interface whose hexadecimal MAC address will be used as the client ID sent with the discover message. Use the **no** form of this command to revert to the default setting.

ip dhcp client client-id *INTERFACE-ID*

no ip dhcp client client-id

Parameters

INTERFACE-ID	Specifies the VLAN interface, whose hexadecimal MAC address will be used as the client ID to be sent with the discover message.

Default

The MAC address of the VLAN will be used as the client ID.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure the hexadecimal MAC address of the specified interface as the client ID sent with the discover message. The specification only applies to the subsequent sending of the DHCP discover messages. The setting only takes effect when the DHCP client is enabled on the interface to acquire the IP address from the DHCP server. One interface can be specified as the client identifier.

Example

This example shows how to configure the MAC address of VLAN 100 as the client ID, sent in the discover message for VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp client client-id vlan 100
Switch(config-if)#
```

15-3 ip dhcp client lease

This command is used to specify the preferred lease time for the IP address to request from the DHCP server. Use the **no** form of this command to disable sending of the lease option.

ip dhcp client lease *DAYS* **[***HOURS* **[***MINUTES***]]**

no ip dhcp client lease

Parameters

DAYS	Specifies the day duration of the lease. The range is from 0 to 10000 days.
HOURS	(Optional) Specifies the hour duration of the lease. The range is from 0 to 23 hours.
MINUTES	(Optional) Specifies the minute duration of the lease. The range is from 0 to 59 minutes.

Default

The lease option is not sent.

Command Mode

Interface Configuration Mode.

Usage Guideline

The setting only takes effect when the DHCP client is enabled to request the IP address for the interface.

Example

This example shows how to get a 5 days release of the IP address.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip address dhcp
Switch(config-if)# ip dhcp client lease 5
Switch(config-if)#
```

16. DHCP Relay Commands

16-1 class (DHCP relay)

This command is used to enter the DHCP pool configuration mode and associate a range of IP addresses with the DHCP class. Use the **no** form of this command to remove the association.

class *NAME*

no class *NAME*

Parameters

NAME	Specifies the DHCP class name with a maximum of 32 characters.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Usage Guideline

In a DHCP relay pool, the user can use this command to associate a DHCP pool class, and then use relay target to set a list of relay target addresses for DHCP packet forwarding. When the client request matches a relay pool which is configured with classes, the client must also match a class configured in the pool in order to be relayed. If there is no class configured in a relay pool, the client will be relayed to the relay destination server specified for the matched relay pool when the client matches the relay pool.

Example

This example shows how to configure a DHCP class, “Service-A”, defined with DHCP Option 60 matching pattern 0x112233 and 0x102030, classified to the relay pool, "pool1", and is associated with relay target "10.2.1.2".

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)# class Service-A
Switch(config-dhcp-pool-class)# relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

16-2 ip dhcp class (DHCP relay)

This command is used to define a DHCP class and enter the DHCP Class Configuration Mode. Use the **no** form of this command to remove a DHCP class.

ip dhcp class *NAME*

no ip dhcp class *NAME*

Parameters

NAME	Specifies the DHCP class name with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the DHCP Class Configuration Mode. In the mode, the user can use the **option hex** command to define the option matching pattern for the DHCP class. When a class has no option hex associated, the class will be matched by any packet.

Example

This example shows how to configure a DHCP class “Service-A” and defined with DHCP Option 60 matching pattern 0x112233.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)#
```

16-3 ip dhcp pool (DHCP Relay)

This command is used to configure a DHCP relay pool on a DHCP relay agent and enter the DHCP pool configuration mode. Use the **no** form of this command to delete a DHCP relay pool.

ip dhcp pool *NAME*

no ip dhcp pool *NAME*

Parameters

NAME	Specifies the address pool name with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

In addition to DHCP relay packets, the relay destination of the DHCP server can be specified in the DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP Pool Configuration Mode, use the **relay source** command to specify the source subnet of the client requests, and use the **relay destination** command to specify the relay destination server address.

When receiving a DHCP request packet, if the subnet that the packet comes from matches the relay source of a relay pool, the packet will be relayed based on the matched relay pool. To relay based on the relay pool, if the

request packet is a relayed packet, the Gateway IP Address (GIADDR) of the packet is the source of the request. If the GIADDR is zero, the subnet of the received interface is the source of the packet.

In a DHCP relay pool, the user can further use the **class** command and the **relay target** command to define the relay target address for the request packets that match the option pattern.

Example

This example shows how to create a DHCP relay pool, called pool1. In the relay pool, the subnet 172.19.18.0/255.255.255.0 is specified as the source subnet. 10.2.1.1 is specified as the relay destination address.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
switch(config-dhcp-pool)# relay destination 10.2.1.1
switch(config-dhcp-pool)#
```

16-4 ip dhcp relay information check

This command is used to enable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet. Use the **no** form of this command to globally disable the check for Option 82.

ip dhcp relay information check

no ip dhcp relay information check

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

The **ip dhcp relay information check** command and the **ip dhcp relay information check-reply** command together determine whether the check function of Option 82 is effective for an interface. If the **ip dhcp relay information check-reply** command is not configured for an interface, the global setting takes effect. If the **ip dhcp relay information check-reply** command is configured for an interface, the interface setting takes effect.

When the check for Option 82 of the reply packet is enabled, the device will check the validity of the Option 82 field in DHCP reply packets it receives from the DHCP server. If the Option 82 field in the received packet is not present or the option is not the original option inserted by the agent (by checking the remote ID sub-option, the relay agent drops the packet. Otherwise, the relay agent removes the Option 82 field and forwards the packet.

If the check is disabled, the packet will be directly forwarded.

Example

This example shows how to enable the global DHCP relay agent check.

```
Switch#configure terminal
Switch(config)# ip dhcp relay information check
switch(config)#
```

16-5 ip dhcp relay information check-reply

This command is used to configure the DHCP relay agent to validate the relay agent information option in the received DHCP reply packet. Use the **no** form of this command to remove the configuration for the interface.

ip dhcp relay information check-reply [none]

no ip dhcp relay information check-reply [none]

Parameters

none	(Optional) Specifies to disable check for Option 82 of the reply packet.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

The **ip dhcp relay information check** command and the **ip dhcp relay information check-reply** command together determine whether the check function of Option 82 is effective for an interface. If the **ip dhcp relay information check-reply** command is not configured for an interface, the global setting takes effect. If the **ip dhcp relay information check-reply** command is configured for an interface, the interface setting takes effect.

When the check for Option 82 of the reply packet is enabled, the device will check the validity of the Option 82 field in DHCP reply packets it receives from the DHCP server. If the Option 82 field in the received packet is not present or the option is not the original option inserted by the agent (by checking the remote ID sub-option, the relay agent drops the packet. Otherwise, the relay agent removes the Option 82 field and forwards the packet.

If the check is disabled, the packet will be directly forwarded.

Example

This example shows how to disable the global DHCP relay agent check but enable the DHCP relay agent check for the VLAN 100. The effect state of the check function for VLAN 100 is enabled.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay information check
switch(config)# interface vlan 100
switch(config-if)# ip dhcp relay information check-reply
```

16-6 ip dhcp relay information option

This command is used to globally enable the insertion of relay agent information (Option 82) during the relay of DHCP request packets. Use the **no** form of this command to globally disable this insert function.

ip dhcp relay information option

no ip dhcp relay information option

Parameters

None.

Default

By default, Option 82 is not inserted.

Command Mode

Global Configuration Mode.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

When DHCP Option 82 is enabled, the DHCP packet received from the client will be inserted with an Option 82 field before being relayed to the server. The DHCP Option 82 contains two sub-options respectively the circuit ID sub-option and remote ID sub-option.

Administrators can use the **ip dhcp relay information option format remote-id** command to specify a user-defined string for the remote ID sub-option.

Example

This example shows how to enable the insertion of Option 82 during the relay of DHCP request packets.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)#
```

16-7 ip dhcp relay information option-insert

This command is used to enable and configure the insertion of Option 82 during the relay of DHCP request packets on the specified interface. Use the **no** form of this command to remove the configuration of the insert function from the interface.

ip dhcp relay information option-insert [none]

no ip dhcp relay information option-insert [none]

Parameters

none	(Optional) Specifies to disable insertion of Option 82 in the relayed packet. Default

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

This command is only available for VLAN interface configuration.

Use this command to configure the insertion of Option 82 during the relay of DHCP request packets on the specified interface. When this command is not configured, the **ip dhcp relay information option** command takes effect.

Example

This example shows how to enable the insertion of Option 82 during the relay of DHCP request packets and disables the insertion of Option 82 for interface VLAN 100. The insertion of Option 82 is disabled for VLAN 100 but enabled for the remaining interfaces.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information option-insert none
switch(config-if)#
```

16-8 ip dhcp relay information policy

This command is used to globally configure the Option 82 re-forwarding policy for the DHCP relay agent. Use the **no** form of this command to revert to the default setting.

ip dhcp relay information policy {drop | keep | replace}

no ip dhcp relay information policy

Parameters

drop	Specifies to discard the packet that already has the relay option.
keep	Specifies that the DHCP requests packet that already has the relay option is left unchanged and directly relayed to the DHCP server.
replace	Specifies that the DHCP request packet that already has the relay option will be replaced by a new option.

Default

By default, this option is **replace**.

Command Mode

Global Configuration Mode.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

Use this command to configure the global policy for the insertion of Option 82 on packets that already have Option 82.

Example

This example shows how to configure the relay agent option re-forwarding policy to keep.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)#
```

16-9 ip dhcp relay information policy-action

This command is used to configure the information re-forwarding policy for the DHCP relay agent on the specified interface. Use the **no** form of this command to remove the configuration for the interface.

ip dhcp relay information policy-action {drop | keep | replace}

no ip dhcp relay information policy-action

Parameters

drop	Specifies to discard the packet that already has the relay option.
keep	Specifies that the DHCP request packet that already has the relay option is left unchanged and directly relayed to the DHCP server.
replace	Specifies that the DHCP request packet that already has the relay option will be replaced by a new option.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

This command is only available for VLAN interface configuration.

Use this command to configure the information re-forwarding policy for the DHCP relay agent on the specified interface. When this command is not configured, the **ip dhcp relay information policy** command takes effect.

Example

This example shows how to configure the relay agent option re-forwarding policy to keep and set the policy to drop for VLAN 100. The effective relay agent option re-forwarding policy for VLAN 100 is drop and for the remaining interfaces are set as keep.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information policy-action drop
Switch(config-if)#
```

16-10 ip dhcp relay information option format remote-id

This command is used to configure the DHCP information remote ID sub-option. Use the **no** form of this command to configure the default remote ID sub-option.

ip dhcp relay information option format remote-id {default | string *SENTENCE* **| vendor2 | vendor3}**

no ip dhcp relay information option format remote-id

Parameters

default	Specifies to use the Switch's system MAC address as the remote ID. The remote ID is formed in the following format: |----------| | a. | b. | c. | d. | e. | |----------| | 2 | 8 | 0 | 6 | MAC Address | |----------|

	`| 1 byte | 1 byte | 1 byte | 1 byte | 6 bytes |` `|----------|`

string *SENTENCE*	Specifies to use a user-defined string as the remote ID. Space characters are allowed in the string. The remote ID option is formed in the following format:
	`|----------|`
	`| a. | b. | c. | d. | e. |`
	`|----------|`
	`| 2 | n+2 | 1 | n | User Defined |`
	`|----------|`
	`| 1 byte | 1 byte | 1 byte | 1 byte | Max. 32 bytes |`
	`|----------|`

vendor2	Specifies to use the vendor 2. If configures, the remote ID option uses the original format:
	`|----------|`
	`| a. | b. | c. |`
	`|----------|`
	`| 2 | n | System Name |`
	`|----------|`
	`| 1 byte | 1 byte | n byte |`
	`|----------|`
	
	a. *Sub-option type:* The number 2 indicates that this is the remote ID.
	b. *Length:* The length of the value.
	c. *Value:* The character string. The system name of the Switch.

vendor3	Specifies to use the vendor 3. If configures, the remote ID option uses the original format:
	`|----------|`
	`| a. | b. | c. |`
	`|--------|--------|----------|`
	`| 2 | n | User Defined |`
	`|--------|--------|----------|`
	`| 1 byte | 1 byte | Max. 251 bytes |`
	`|----------|`
	
	a. *Sub-option type:* The number 2 indicates that this is the remote ID.
	b. *Length:* Total length of user-defined string. By default, Length is 0 and no value field.
	c. *Value:* Flexible user-defined string that configured through the **ip dhcp relay information option format-type remote-id vendor3 string** *STRING* command. The maximum length is 32.

Default

The Switch's system MAC address is used as the remote ID string.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to select different vendor’s remote ID format or configures a user-defined string of ASCII characters to be the remote ID.

Example

This example shows how to use vendor2 as the remote ID.

```
Switch# Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id vendor2
Switch(config)#
```

This example shows how to configure a user-defined string “switch1” as the remote ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format remote-id string switch1
Switch(config)#
```

16-11 ip dhcp relay information option format-type remote-id

This command is used to configure the DHCP information remote ID sub-option of vendor format string in the Interface Configuration Mode. Use the **no** form of this command to remove the remote ID sub-option of vendor format string.

ip dhcp relay information option format-type remote-id vendor3 string *STRING*

no ip dhcp relay information option format-type remote-id vendor3

Parameters

vendor3	Specifies the vendor 3 user-defined string with the maximum 32 characters.
STRING	Specifies the user-defined string.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to configure each interface’s vendor defined string for option 82 information remote-id sub-option.

Example

This example shows how to define vendor3 remote-id format string as “switch1” on port 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp relay information option format-type remote-id vendor3 string
switch1
Switch(config-if)#
```

16-12 ip dhcp relay information option format circuit-id

This command is used to configure the DHCP information circuit ID sub-option. Use the **no** form of this command to configure the default circuit ID sub-option.

ip dhcp relay information option format circuit-id {default | string *SENTENCE* **| vendor1 | vendor2| vendor3| vendor4 | vendor5 | vendor6}**

no ip dhcp relay information option format circuit-id

Parameters

default — Specifies to use the default circuit ID sub-option. If configured, the circuit ID will use the original format:

a.	b.	c.	d.	e.	f.	g.
1	0x6	0	4	VLAN	Module ID	Port ID
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. *Sub-option type*: The number 1 indicates that this is the circuit ID.
b. *Length*: The length of the value. This should be 6.
c. *Circuit ID's sub-option*: This should be 0.
d. *Sub-option's length*: This should be 4.
e. The VLAN ID (S-VID).
f. *Module ID*: For stand-alone switch this is 0.
g. *Port ID*: Port number for each box.

string *SENTENCE* — Specifies to use a user-defined string as the circuit ID. Space characters are allowed in the string.

a.	b.	c.	d.	e.
2	n+2	1	n	User Defined
1 byte	1 byte	1 byte	1 byte	Max. 32 bytes

vendor1 — If configured, the circuit ID will use the following format to communicate with the server:

a.	b.	c.	d.	e.	f.
1	0x10	0	6	VLAN	Slot ID
1 byte	1 byte	1 byte	1 byte	2 bytes	2 bytes

g.	h.	i.	j
Port ID	1	6	MAC
2 bytes	1 byte	1 byte	6 bytes

a. *Sub-option type:* 1 means circuit ID.
b. *Length*.

	c. *Circuit ID's sub-option's first tag:* This should be 0. **d.** *First tag's length:* This should be 6 **e.** *VLAN ID*. **f.** *Slot ID:* For a stand-alone switch, this is 1. **g.** *Port ID:* The port number of each box. **h.** *Circuit ID's sub-option's second tag:* This should be 1. **i.** *Second tag's length:* This should be 6. **j.** *MAC address:* The Switch's system MAC address.
vendor2	Specifies to use vender2.
vendor3	Specifies to use vender3.
vendor4	Specifies to use vender4.
vendor5	Specifies to use vender5.
vendor6	Specifies to use vender6.

Default

The circuit ID format is VLAN ID, module number and port number.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to select different vendor's circuit ID format or configures a user-defined string of ASCII characters to be the circuit ID.

Example

This example shows how to use vendor1 as the circuit ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id vendor1
Switch(config)#
```

This example shows how to configure a user-defined string "abcd" as the circuit ID.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information option
Switch(config)# ip dhcp relay information option format circuit-id string abcd
Switch(config)#
```

16-13 ip dhcp relay information option format-type circuit-id

This command is used to configure the Option 82 information circuit ID in the user-defined string for different vendors on the specified interface. Use the **no** form of this command to remove the Option 82 information circuit ID.

ip dhcp relay information option format-type circuit-id vendor3 string *STRING*

no ip dhcp relay information option format-type circuit-id vendor3 string

Parameters

vendor3	Specifies to the vender3 user-defined string with the maximum 32 characters.
STRING	Specifies the vendor-defined string.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to configure the Option 82 information circuit ID in the user-defined string for different vendors on the specified interface.

Example

This example shows how to define vendor3 circuit-id of “abc” on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id vendor3 string abc
Switch(config-if)#
```

16-14 ip dhcp relay information trust-all

This command is used to enable the DHCP relay agent to trust the IP DHCP relay information for all interfaces. Use the **no** form of this command to disable the trusting on all interfaces.

ip dhcp relay information trust-all

no ip dhcp relay information trust-all

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

When IP DHCP relay information trust is enabled on an interface, the arriving packets with a GIADDR of 0 (this relay agent is the first relay of this DHCP request packet) but with relay agent information option present will be accepted. If it is not trusted, these packets will be dropped.

When this command is enabled, IP DHCP relay information is trusted for all interfaces. When this command is disabled, the trust state is determined by the **ip dhcp relay information trusted** command in the Interface Configuration Mode.

Use the **show ip dhcp relay information trusted-sources** command to see the settings.

Example

This example shows how to enable the DHCP relay agent to trust IP DHCP relay information for all interfaces.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information trust-all
Switch(config)#
```

16-15 ip dhcp relay information trusted

This command is used to enable the DHCP relay agent to trust the relay information for the interface. Use the **no** form of this command to disable the trusting of relay information for the interface.

ip dhcp relay information trusted

no ip dhcp relay information trusted

Parameters

None.

Default

By default, information is not trusted.

Command Mode

Interface Configuration Mode.

Usage Guideline

When IP DHCP relay information trust is enabled on an interface, the arriving packets with a GIADDR of 0 (this relay agent is the first relay of this DHCP request packet) but with relay agent information option present will be accepted. If it is not trusted, these packets will be dropped.

When the **ip dhcp relay information trust-all** command is enabled, IP DHCP relay information is trusted for all interfaces. When the **ip dhcp relay information trust-all** command is disabled, the trust state is determined by this command.

Use the **show ip dhcp relay information trusted-sources** command to see the settings.

Example

This example shows how to disable the DHCP relay agent to trust all interface settings and enable trust for VLAN 100.

```
Switch# configure terminal
Switch(config)# no ip dhcp relay information trust-all
Switch(config)# interface vlan 100
Switch(config-if)# ip dhcp relay information trusted
Switch(config-if)#
```

16-16 ip dhcp local-relay vlan

This command is used to enable local relay on a VLAN or a group of VLANs. Use the **no** form of this command to disable the local relay function.

ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

no ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the VLAN used.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The local relay relays the DHCP message to all local VLAN member ports based on the relay option setting. The local relay does not change the destination IP, destination MAC, and the gateway field of the packet.

Example

This example shows how to enable the local relay function on VLAN 100.

```
Switch# configure terminal
Switch(config)# ip dhcp local-relay vlan 100
Switch(config)#
```

16-17 option hex (DHCP relay)

This command is used to specify a DHCP option matching pattern for a DHCP class. Use the **no** form of this command to delete the specified matching pattern for a DHCP class.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Parameters

CODE	Specifies the DHCP option number.
PATTERN	Specifies the hex pattern of the specified DHCP option.
*	(Optional) Specifies not to match the remaining bits of the option. If not specified, the bit length of the PATTERN should be the same as the bit length of the option.
MASK	(Optional) Specifies the hex bit mask for masking of the pattern. The masked pattern bits will be matched. If not specified, all bits specified by PATTERN will be checked. The bit set to FF will be checked. The input format should be the same as PATTERN.

Default

None.

Command Mode

DHCP Class Configuration Mode.

Usage Guideline

Use the **ip dhcp class command** with this command to define a DHCP class. The classes in a pool are matched in the sequence of the class configuration in a pool.

Use the **option hex** command to specify the DHCP option code number with its matching pattern for a DHCP class. Multiple option patterns can be specified for a DHCP class. If the packet matches any of the specified pattern of a DHCP class, the packet will be classified to the DHCP class and forwarded based on the specified target.

The following are some common used option codes:

- **Option 60** - Vendor class identifier.
- **Option 61** - Client identifier.
- **Option 77** - User class.
- **Option 124** - Vendor-identifying vendor class.
- **Option 125** - Vendor-identifying vendor-specific information.

Example

This example shows how to configure a DHCP class “Service-A” and defined with DHCP Option 60 matching pattern 0x112233 and 0x102030.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)#
```

16-18 relay destination

This command is used to specify the DHCP relay destination IP address associated with a relay pool. Use the **no** form of this command to delete a DHCP relay destination from the DHCP relay pool.

relay destination *IP-ADDRESS*

no relay destination *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the relay destination DHCP server IP address.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Usage Guideline

The relay destination of the DHCP server can be specified in the DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP Pool Configuration Mode and then use the **relay source** command to specify the source subnet of the client requests. Use the **relay destination** command to specify the relay destination server address. Multiple relay sources and multiple relay destinations can be specified in a pool. If a packet matches any of the relay sources, the packet will be forwarded to all of the relay destinations.

When receiving a DHCP request packet, if the subnet of the received packet matches the relay source of a relay pool, the packet will be relayed based on this relay pool. To relay a packet based on the relay pool, if the request packet is a relayed packet, the GIADDR of the packet is the source of the request. If the request packet is not a relayed packet, the subnet of the received interface is the source of the packet.

In a DHCP relay pool, administrators can further use the **class** command and the **relay target** command to associate a list of relay target addresses with a DHCP class.

Example

This example shows how to create a DHCP relay pool, called pool1. In the relay pool, the subnet 172.19.10.0/255.255.255.0 is specified as the source subnet. 10.2.1.1 is specified as the relay destination address.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.10.0 255.255.255.0
Switch(config-dhcp-pool)# relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

16-19 relay source

This command is used to specify the source subnet of client packets. Use the **no** form of this command to remove the source subnet

relay source *IP-ADDRESS SUBNET-MASK*

no relay source *IP-ADDRESS SUBNET-MASK*

Parameters

IP-ADDRESS	Specifies the source subnet of client packets.
SUBNET-MASK	Specifies the network mask of the source subnet.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Usage Guideline

The relay destination of the DHCP server can be specified in the DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP Pool Configuration Mode and then use the **relay source** command to specify the source subnet of the client requests. Use the **relay destination** command to specify the relay destination server address. Multiple relay sources and multiple relay destinations can be specified in a pool. If a packet matches any of the relay sources, the packet will be forwarded to all of the relay destinations.

When receiving a DHCP request packet, if the subnet of the received packet matches the relay source of a relay pool, the packet will be relayed based on this relay pool. To relay a packet based on the relay pool, if the request packet is a relayed packet, the GIADDR of the packet is the source of the request. If the request packet is not a relayed packet, the subnet of the received interface is the source of the packet.

In a DHCP relay pool, administrators can further use the **class** command and the **relay target** command to associate a list of relay target addresses with a DHCP class. The DHCP packet will not be relayed when the interface that receives the packet has no IP address configured.

Example

This example shows how to create a DHCP relay pool, called pool2. In the relay pool, the subnet 172.19.18.0/255.255.255.0 is specified as the source subnet and 10.2.1.10 is specified as the relay destination address.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool2
Switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)# relay destination 10.2.1.10
Switch(config-dhcp-pool)#
```

16-20 relay target

This command is used to specify a DHCP relay target for relaying packets that matches the value pattern of the option defined in the class. Use the **no** form of this command to delete a relay target.

relay target *IP-ADDRESS*

no relay target *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the relay target server IP address for the class.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Usage Guideline

In a DHCP relay pool, administrators can further use the **class** command and the **relay target** command to associate a list of relay target addresses with a DHCP class. When the client request matches a relay pool and the DHCP relay pool is defined with classes, the client request must match a class specified in the pool in order to be relayed. If the packet does not match any class in the pool, the packet will not be replayed. If the matched relay pool has no class defined, the request will be relayed to the relay destination of the matched relay pool. Multiple **relay target** commands can be specified for a class. If a packet matches the class, the packet will be forwarded to all of the relay targets.

If the **relay target** command is not configured for a class, the relay target follows the relay destination specified for the pool. The DHCP packet will not be relayed when the interface that receives the packet has no IP address configured.

Example

This example shows how to configure a DHCP relay target for relaying packets that matches the value pattern of the option defined in the class.

```
Switch# configure terminal
Switch(config)# ip dhcp class Service-A
Switch(config-dhcp-class)# option 60 hex 112233
Switch(config-dhcp-class)# option 60 hex 102030
Switch(config-dhcp-class)#exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)# class Service-A
Switch(config-dhcp-pool-class)# relay target 10.2.1.2
Switch(config-dhcp-pool-class)#
```

16-21 service dhcp

This command is used to enable the DHCP relay service on the Switch. Use the **no** form of this command to disable the DHCP relay service.

service dhcp

no service dhcp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the DHCP relay service on the switch.

Example

This example shows how to disable the DHCP relay service.

```
Switch# configure terminal
Switch(config)#no service dhcp
Switch(config)#
```

16-22 show ip dhcp relay information trusted-sources

This command is used to display all interfaces configured as trusted sources for the DHCP relay information option.

show ip dhcp relay information trusted-sources

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the effective setting of the trust relay information option function.

Example

This example shows how to display the effective setting of the trust relay information option function when the **ip dhcp relay information trust-all** command is disabled.

```
Switch# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan100             vlan200             vlan300             vlan400
vlan500

Total Entries: 5

Switch#
```

This example shows how to display the effective setting of the trust relay information option function when the **ip dhcp relay information trust-all** command is enabled.

```
Switch# show ip dhcp relay information trusted-sources

All interfaces are trusted source of relay agent information option

Switch#
```

16-23 show ip dhcp relay information option format-type

This command is used to display the interface option format configuration.

show ip dhcp relay information option format-type [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display information related to the interface specified here.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the interface option format configuration. If no parameter is specified, information of all interfaces will be displayed.

Example

This example shows how to display the interface option format configuration.

```
Switch#show ip dhcp relay information option format-type

eth1/0/1
Remote ID vendor string: string1
eth1/0/2
Circuit ID vendor string: string1
eth1/0/3
Remote ID vendor string: string3
Circuit ID vendor string: string4

Total Entries: 3

Switch#
```

16-24 show ip dhcp relay information option-insert

This command is used to display the relay option insert configuration.

show ip dhcp relay information option-insert

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display relay information options with insert configuration information.

Example

This example shows how to display relay information Option 82 option and insert configuration information for all VLANs.

```
Switch# show ip dhcp relay information option-insert

Interface     Option-Insert
------------ ----------
vlan1         Enabled
vlan2         Disabled
vlan3         Not Configured

Total Entries: 3

Switch#
```

16-25 show ip dhcp relay information policy-action

This command is used to display the relay option policy action configuration.

show ip dhcp relay information policy-action

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the relay information option policy action configuration information.

Example

This example shows how to display relay information Option 82 policy action configuration information for all VLANs.

```
Switch# show ip dhcp relay information policy-action

Interface      Policy
------------ ----------
vlan1          Keep
vlan2          Drop
vlan3          Replace
vlan4          Not configured

Total Entries: 4

Switch#
```

17. DHCP Server Screening Commands

17-1 based-on hardware-address

This command is used to add an entry of the DHCP server screen profile. Use the **no** form of this command to delete the specified entry.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Parameters

CLIENT-HARDWARE-ADDRESS	Specifies the MAC address of the client.

Default

None.

Command Mode

DHCP Server Screen Configure Mode.

Usage Guideline

The server message with the specified server IP address and client address in the payload will be permitted. These binding entries restrict that only specific servers are allowed to offer addresses to service specific clients.

Example

This example shows how to configure a DHCP server screen profile named “campus-profile” which contains a list of MAC addresses of clients.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#
```

17-2 clear ip dhcp snooping server-screen log

This command is used to clear the server screen log buffer.

clear ip dhcp snooping server-screen log

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Usage Guideline

Use this command to clear the server screen log buffer. The DHCP server screen log buffer keeps tracks the information of packet that does not pass the screening. The first packet that violates the check will be sent to log module and recorded in the server screen log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared.

Example

This example shows how to clear the server screen log.

```
Switch# clear ip dhcp snooping server-screen log
Switch#
```

17-3 dhcp-server-screen profile

This command is used to define a server screen profile and enter the DHCP Server Screen Configure Mode. Use the **no** form of this command to delete the specified server screen profile.

dhcp-server-screen profile *PROFILE-NAME*

no dhcp-server-screen profile *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the profile name with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the DHCP Server Screen Configure Mode to define a server screen profile. The profile can be used to define the DHCP server screen entry.

Example

This example shows how to enter the DHCP Server Screen Configure Mode to define the profile “campus”.

```
Switch# configure terminal
Switch(config)# service dhcp
Switch(config)# dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

17-4 ip dhcp snooping server-screen

This command is used to enable DHCP server screening. Use the **no** form of this command to disable it.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **profile** *PROFILE-NAME***]**

no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS***]**

Parameters

SERVER-IP-ADDRESS	(Optional) Specifies the trust DHCP sever IP address.
profile *PROFILE-NAME*	(Optional) Specifies the profile with the client MAC address list for the DHCP sever.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

The DHCP server screening function is used to filter the DHCP server packets on the specific interface and receive the trust packets from the specific source. This feature can make a protected network usable when a malicious host sends DHCP server packets.

If the server IP address is not specified, it will enabled or disabled the DHCP server screen on the interface. By default, the DHCP server screen is disabled on all interfaces. If enabled, the DHCP server screen, on a specific interface, will filter all DHCP server packets from the interface and only forward trusted server packets.

If a server screen entry is defined with a profile that contains a client MAC address, the server message with the server IP address and the client addresses contained in the profile is forwarded.

If an entry is defined without the client's MAC address, the server message with the specified server IP address will be forwarded. Each server can only have one corresponding entry in the table.

If the entry is defined with a profile but the entry does not exist, messages with the server IP specified by the entry are not forwarded.

Example

This example shows how to configure a DHCP server screen profile named "campus-profile" and associate it with a DHCP server screen entry on port 3.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

17-5 ip dhcp snooping server-screen log-buffer

This command is used to configure the DHCP server screen log buffer parameter. Use the **no** form of this command to revert to the default setting.

ip dhcp snooping server-screen log-buffer entries *NUMBER*

no ip dhcp snooping server-screen log-buffer entries

Parameters

NUMBER	Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the maximum entry number of the log buffer. The DHCP server screen log buffer keeps tracks of the information of packets that did not pass the screening. The first packet that violates the check will be sent to the log module and recorded in the server screen log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared.

If the log buffer is full but more violation events occur, packets will be discarded but the event will not be sent to the syslog module. If the user specifies a buffer size less than the current entry number, the log buffer will automatically be cleared.

Example

This example shows how to change the maximum buffer number to 64.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

17-6 show ip dhcp server-screen log

This command is used to display the server screen log buffer.

show ip dhcp server-screen log

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the content of the DHCP server screen log buffer. The buffer keeps the information of server messages that violates the screening. The number of occurrences of the same violation and the latest time of the occurrence are tracked.

Example

This example shows how to display the DHCP server screen log buffer.

```
Switch# show ip dhcp server-screen log

Total log buffer size: 64

VLAN           Server IP                Client MAC                Occurrence
---------- ------------------- --------------------- ----------------------------

100             10.20.1.1               00-20-30-40-50-60       06:30:37, 2013-02-07
100             10.58.2.30              10-22-33-44-50-60       06:31:42, 2013-02-07

Total Entries: 2

Switch#
```

17-7 snmp-server enable traps dhcp-server-screen

This command is used to enable the sending of SNMP notifications for forged DHCP server attacking. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps dhcp-server-screen

no snmp-server enable traps dhcp-server-screen

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

When DHCP server screening is enabled and if the Switch received a forged DHCP server packet, the Switch will log the event if any attack packet is received. Use this command to enable or disable the sending of SNMP notifications for such events.

Example

This example shows how to enable the sending of traps for DHCP server screening.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps dhcp-server-screen
Switch(config)#
```

18. DHCP Snooping Commands

18-1 ip dhcp snooping

This command is used to globally enable DHCP snooping. Use the **no** form of this command to disable DHCP snooping.

ip dhcp snooping

no ip dhcp snooping

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The DHCP snooping function snoops the DHCP packets arriving at the untrusted interface on the VLAN that is enabled for DHCP snooping. With this function, the DHCP packets that come from the untrusted interface can be validated and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

Example

This example shows how to enable DHCP snooping.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)#
```

18-2 ip dhcp snooping information option allow-untrusted

This command is used to globally allow DHCP packets with the relay Option 82 on the untrusted interface. Use the **no** form of this command to not allow packets with the relay Option 82.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Parameters

None.

Default

By default, this option is not allowed.

Command Mode

Global Configuration Mode.

Usage Guideline

The DHCP snooping function validates the DHCP packets when it arrives at the port on the VLAN that is enabled for DHCP snooping. By default, the validation process will drop the packet if the gateway address is not equal to 0 or Option 82 is present.

Use this command to allow or deny packets with the relay Option 82 arriving at the untrusted interface.

Example

This example shows how to enable DHCP snooping for Option 82 to allow untrusted ports.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping information option allow-untrusted
Switch(config)#
```

18-3 ip dhcp snooping database

This command is used to configure the storing of DHCP snooping binding entries to a remote site. Use the no form of this command to disable the storing or reset the parameters to the default setting.

ip dhcp snooping database {*URL* **| write-delay** *SECONDS***}**

no ip dhcp snooping database [write-delay]

Parameters

URL	Specifies the URL in the following form: ● tftp://location/filename
write-delay *SECONDS*	Specifies the time delay to write the entries after a change is seen in the binding entry. The default is 300 seconds. The range is from 60 to 86400.

Default

By default, the URL for the database agent is not defined.

The write delay value is set to 300 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to store the DHCP binding entry to a remote server. Use the follow method to store DHCP binding entries:

- tftp: Store the entries to remote site via TFTP.

The lease time of the entry will not be modified and the live time will continue to be counted while the entry is provisioned.

Example

This example shows how to store the binding entry to a file in the file system.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

18-4 clear ip dhcp snooping database statistics

This command is used to clear the DHCP binding database statistics.

clear ip dhcp snooping database statistics

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the DHCP binding database statistics.

Example

This example shows how to clear the snooping database statistics.

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

18-5 clear ip dhcp snooping binding

This command is used to clear the DHCP binding entry.

clear ip dhcp snooping binding [*MAC-ADDRESS***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***]**

Parameters

MAC-ADDRESS	(Optional) Specifies the MAC address to clear.
IP-ADDRESS	(Optional) Specifies the IP address to clear.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to clear.
interface *INTERFACE-ID*	(Optional) Specifies the interface to clear.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the DHCP binding entry, including the manually configured binding entry.

Example

This example shows how to clear all snooping binding entries.

```
Switch# clear ip dhcp snooping binding
Switch#
```

18-6 renew ip dhcp snooping database

This command is used to renew the DHCP binding database.

renew ip dhcp snooping database *URL*

Parameters

URL	Specifies the URL in the following form: ● tftp://location/filename

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to load the bind entry database from a URL and add the entries to the DHCP snooping binding entry table.

Example

This example shows how to renew the DHCP snooping binding database.

```
Switch# renew ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch#
```

18-7 ip dhcp snooping binding

This command is used to manually configure a DHCP snooping entry.

ip dhcp snooping binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

Parameters

MAC-ADDRESS	Specifies the MAC address of the entry.
vlan *VLAN-ID*	Specifies the VLAN of the entry.
IP-ADDRESS	Specifies the IP address of the entry.
INTERFACE-ID	Specifies the interfaces to be configured
SECONDS	Specifies the interval after which bindings are no longer valid. This value must be between 60 and 4294967295 seconds.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to create a dynamic DHCP snooping entry.

Example

This example shows how to configure a DHCP snooping entry with IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 and port 10 with an expiry time of 100 seconds.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10 expiry 100
Switch#
```

18-8 ip dhcp snooping trust

This command is used to configure a port as a trusted interface for DHCP snooping. Use the **no** form of this command to revert to the default setting.

ip dhcp snooping trust

no ip dhcp snooping trust

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Ports connected to the DHCP server or to other switches should be configured as trusted interfaces. The ports connected to DHCP clients should be configured as untrusted interfaces. DHCP snooping acts as a firewall between untrusted interfaces and DHCP servers.

When a port is configured as a untrusted interface, the DHCP message arrives at the port on a VLAN that is enabled for DHCP snooping. The Switch forwards the DHCP packet unless any of the following conditions occur (in which case the packet is dropped):

- The Switch port receives a packet (such as a DHCPOFFER, DHCPACK, or DHCPNAK packet) from a DHCP server outside the firewall.
- If **ip dhcp snooping verify mac-address** is enabled, the source MAC in the Ethernet header must be the same as the DHCP client hardware address to pass the validation.
- The untrusted interface receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0 or the relay agent forward a packet that includes Option 82 to an untrusted interface.

- The router receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.

In addition to doing the validation, DHCP snooping also create a binding entry based on the IP address assigned to client by the server in DHCP snooping binding database. The binding entry contains information including MAC address, IP address, the VLAN ID and port ID where the client is located, and the expiry of the lease time.

Example

This example shows how to enable DHCP snooping trust for port 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

18-9 ip dhcp snooping limit entries

This command is used to configure the number of the DHCP snooping binding entries that an interface can learn. Use the **no** form of this command to reset the DHCP message entry limit.

ip dhcp snooping limit entries *NUMBER*

no ip dhcp snooping limit entries

Parameters

NUMBER	Specifies the number of DHCP snooping binding entries limited on a port. The range of value is from 0 to 1024.

Default

By default, this option is no-limit.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration. This command only takes effect on untrusted interfaces. The system will stop learning binding entries associated with the port if the maximums number is exceeded.

Example

This example shows how to configure the limit on binding entries allowed on port 1 to 100.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ip dhcp snooping limit entries 100
Switch(config-if)#
```

18-10 ip dhcp snooping limit rate

This command is used to configure the number of the DHCP messages that an interface can receive per second. Use the **no** form of this command to reset the DHCP message rate limiting.

ip dhcp snooping limit rate *VALUE*

no ip dhcp snooping limit rate

Parameters

VALUE	Specifies the number of DHCP messages that can be processed per second. The valid range is from 1 to 300.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

When the rate of the DHCP packet exceeds the limitation, the port will be changed to the error disable state.

Example

This example shows how to configure number of DHCP messages that a switch can receive per second on port 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)#
```

18-11 ip dhcp snooping station-move deny

This command is used to disable the DHCP snooping station move state. Use the **no** form of this command to enable the DHCP snooping roaming state.

ip dhcp snooping station-move deny

no ip dhcp snooping station-move deny

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

hen DHCP snooping station move is enabled, the dynamic DHCP snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if it detects that a new DHCP process belong to the same VLAN ID and MAC address.

Example

This example shows how to disable the roaming state.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10
Switch(config)# ip dhcp snooping station-move deny
Switch(config)#
```

18-12 ip dhcp snooping verify mac-address

This command is used to enable the verification that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to disable the verification of the MAC address.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The DHCP snooping function validates the DHCP packets when they arrive at the port on the VLAN that is enabled for DHCP snooping. By default, DHCP snooping will verify that the source MAC address in the Ethernet header is the same as the DHCP client hardware address to pass the validation.

Example

This example shows how to enable the verification that the source MAC address in a DHCP packet matches the client hardware address.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping verify mac-address
Switch(config)#
```

18-13 ip dhcp snooping vlan

This command is used to enable DHCP snooping on a VLAN or a group of VLANs. Use the **no** form of this command to disable DHCP snooping on a VLAN or a group of VLANs.

ip dhcp snooping vlan VLAN-ID [, | -]

no ip dhcp snooping vlan VLAN-ID [, | -]

Parameters

VLAN-ID	Specifies the VLAN to be used.

,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, DHCP snooping is enabled on all VLANs.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to globally enable DHCP snooping and use the **ip dhcp snooping vlan** command to enable DHCP snooping for a VLAN. The DHCP snooping function snoops the DHCP packets arriving at the untrusted interface on VLAN that is enabled for DHCP snooping. With this function, the DHCP packets come from the untrusted interface can be validated and a DHCP binding database will be constructed for the DHCP snooping enabled VLAN. The binding database provides IP and MAC binding information that can be further used by the IP source guard and dynamic ARP inspection process.

Example

This example shows how to enable DHCP snooping on VLAN 10.

```
Switch#configure terminal
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

This example shows how to disable DHCP snooping on a range of VLANs.

```
Switch#configure terminal
Switch(config)# no ip dhcp snooping vlan 10,15-18
Switch(config)#
```

18-14 show ip dhcp snooping

This command is used to display the DHCP snooping configuration.

show ip dhcp snooping

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display DHCP snooping configuration settings.

Example

This example shows how to display DHCP snooping configuration settings.

```
Switch# show ip dhcp snooping

DHCP Snooping is disabled
DHCP Snooping is enabled on VLANs:
     1-4094
Verification of MAC address is enabled
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted   Rate Limit   Entry Limit
-------------- --------- ------------ ------------
eth1/0/1       no        10           no_limit
eth1/0/2       no        no_limit     no_limit
eth1/0/3       no        no_limit     no_limit
eth1/0/4       no        no_limit     no_limit
eth1/0/5       no        no_limit     no_limit
eth1/0/6       no        no_limit     no_limit
eth1/0/7       no        no_limit     no_limit
eth1/0/8       no        50           20
eth1/0/9       yes       no_limit     no_limit
eth1/0/10      no        no_limit     no_limit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

18-15 show ip dhcp snooping binding

This command is used to display DHCP snooping binding entries.

show ip dhcp snooping binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [vlan** *VLAN-ID***] [interface [***INTERFACE-ID* **[, | -]]]**

Parameters

IP-ADDRESS	(Optional) Specifies to display the binding entry based on the IP address.
MAC-ADDRESS	(Optional) Specifies to display the binding entry based on the MAC address.
vlan *VLAN-ID*	(Optional) Specifies to display the binding entry based on the VLAN.
interface	(Optional) Specifies to display the binding entry based on the port ID.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

EXEC Mode.

Usage Guideline

Use this command to display DHCP snooping binding entries.

Example

This example shows how to display DHCP snooping binding entries.

```
Switch# show ip dhcp snooping binding

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.10.

```
Switch# show ip dhcp snooping binding 10.1.1.10

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.10 and MAC 00-01-02-00-00-05.

```
Switch# show ip dhcp snooping binding 10.1.1.10 00-01-02-03-04-05

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.10 and MAC 00-01-02-03-04-05 on VLAN 100.

```
Switch# show ip dhcp snooping binding 10.1.1.10 00-01-02-03-04-05 vlan 100

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ------------- ---- -------------
00-01-02-03-04-05 10.1.1.10       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by VLAN 100.

```
Switch# show ip dhcp snooping binding vlan 100

MAC Address       IP Address      Lease(seconds) Type        VLAN Interface
----------------- --------------- -------------- ------------ ---- -------------
00-01-02-03-04-05 10.1.1.10       1500         dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495         dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries on port 5.

```
Switch# show ip dhcp snooping binding interface eth1/0/5

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------ ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       495            dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

Display Parameters

MAC Address	The client hardware MAC address.
IP Address	The client IP address assigned from the DHCP server.
Lease (seconds)	The IP address lease time.
Type	The Binding type configured from the CLI or dynamically learned.
VLAN	The VLAN ID.
Interface	The interface that connects to the DHCP client host.

18-16 show ip dhcp snooping database

This command is used to display the statistics of the DHCP snooping database.

show ip dhcp snooping database

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display DHCP snooping database statistics.

Example

This example shows how to display DHCP snooping database statistics.

```
Switch#show ip dhcp snooping database

URL: tftp://10.0.0.2/store/dhcp-snp-bind
Write Delay Time: 300 seconds

Last ignored bindings counters:
Binding collisions :   0         Expired    lease  :   0
Invalid interfaces :   0         Unsupported vlans :   0
Parse failures     :   0         Checksum errors   :   0

Switch#
```

Display Parameters

Binding Collisions	The number of entries that created collisions with exiting entries in DHCP snooping database.
Expired leases	The number of entries that expired in the DHCP snooping database.
Invalid interfaces	The number of interfaces that received the DHCP message but DHCP snooping is not performed.
Parse failures	The number of illegal DHCP packets.
Checksum errors	The number of calculated checksum values that is not equal to the stored checksum.
Unsupported vlans	The number of the entries of which the VLAN is disabled.

18-17 clear ip dhcp snooping server-screen log

This command is used to clear the server screen log buffer.

clear ip dhcp snooping server-screen log

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the server screen log buffer. The DHCP server screen log buffer keeps tracks the information of packet that does not pass the screening. The first packet that violates the check will be sent to log module and recorded in the server screen log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared.

Example

This example shows how to clear the server screen log.

```
Switch# clear ip dhcp snooping server-screen log
Switch#
```

18-18 dhcp-server-screen profile

This command is used to define a server screen profile and enter the DHCP Server Screen Configure Mode. Use the **no** form of this command to delete the specified server screen profile.

dhcp-server-screen profile *PROFILE-NAME*

no dhcp-server-screen profile *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the profile name with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the DHCP Server Screen Configure Mode to define a server screen profile. The profile can be used to define the DHCP server screen entry.

Example

This example shows how to enter the DHCP Server Screen Configure Mode to define the profile “campus”.

```
Switch# configure terminal
Switch(config)# service dhcp
switch(config)# dhcp-server-screen profile campus
switch(config-dhcp-server-screen)#
```

18-19 ip dhcp snooping server-screen

This command is used to enable DHCP server screening. Use the **no** form of this command to disable it.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **[profile** *PROFILE-NAME***]]**

no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS***]**

Parameters

SERVER-IP-ADDRESS	(Optional) Specifies the trust DHCP sever IP address.
profile *PROFILE-NAME*	(Optional) Specifies the profile with the client MAC address list for the DHCP sever.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

The DHCP server screening function is used to filter the DHCP server packets on the specific interface and receive the trust packets from the specific source. This feature can make a protected network usable when a malicious host sends DHCP server packets.

If the server IP address is not specified, it will enabled or disabled the DHCP server screen on the interface. By default, the DHCP server screen is disabled on all interfaces. If enabled, the DHCP server screen, on a specific interface, will filter all DHCP server packets from the interface and only forward trusted server packets.

If a server screen entry is defined with a profile that contains a client MAC address, then the server message with the server IP address and the client addresses contained in the profile is forwarded.

If an entry is defined without the client's MAC address, then the server message with the specified server IP address will be forwarded. Each server can only have one corresponding entry in the table.

If the entry is defined with a profile but the entry does not exist, then messages with the server IP specified by the entry are not forwarded.

Example

This example shows how to configure a DHCP server screen profile named "campus-profile" and associate it with a DHCP server screen entry on port 3.

```
Switch# configure terminal
Switch(config)# dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)# based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

18-20 ip dhcp snooping server-screen log-buffer

This command is used to configure the DHCP server screen log buffer parameter. Use the **no** form of this command to revert to the default setting.

ip dhcp snooping server-screen log-buffer entries *NUMBER*

no ip dhcp snooping server-screen log-buffer entries

Parameters

NUMBER	Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the maximum entry number of the log buffer. The DHCP server screen log buffer keeps tracks of the information of packets that did not pass the screening. The first packet that violates the check will be sent to the log module and recorded in the server screen log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared.

If the log buffer is full but more violation events occur, packets will be discarded but the event will not be sent to the syslog module. If the user specifies a buffer size less than the current entry number, then the log buffer will automatically be cleared.

Example

This example shows how to change the maximum buffer number to 64.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping server-screen log-buffer entries 64
Switch(config)#
```

18-21 show ip dhcp server-screen log

This command is used to isplay the server screen log buffer.

show ip dhcp server-screen log

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the content of the DHCP server screen log buffer. The buffer keeps the information of server messages that violates the screening. The number of occurrences of the same violation and the latest time of the occurrence are tracked.

Example

This example shows how to display the DHCP server screen log buffer.

```
Switch# show ip dhcp server-screen log
Total log buffer size: 64

VLAN   Server IP       Client MAC        Occurrence
------ --------------- ----------------- ----------------------
100    10.20.1.1       00-20-30-40-50-60 06:30:37, 2014-03-10
100    10.58.2.30      10-22-33-44-50-60 06:31:42, 2014-03-10

Total Entries: 2

Switch#
```

19. DHCPv6 Client Commands

19-1 clear ipv6 dhcp client

This command is used to restart the DHCPv6 client on an interface.

clear ipv6 dhcp client *INTERFACE-ID*

Parameters

INTERFACE-ID	Specifies the VLAN interface to restart the DHCPv6 client.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for VLAN interface configuration.

Use this command to restart the IPv6 DHCP client on the specified interface.

Example

This example shows how to restart the DHCPv6 client for VLAN 1.

```
Switch# clear ipv6 dhcp client vlan1
Switch#
```

19-2 show ipv6 dhcp

This command is used to display the DHCPv6 related settings on the interface.

show ipv6 dhcp [interface [*INTERFACE-ID***]]**

Parameters

INTERFACE-ID	(Optional) Specifies the VLAN interface to display the DHCPv6 related settings.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use the **show ipv6 dhcp** command to display the device's DHCPv6 DUID.

Use the **show ipv6 dhcp interface** command to display DHCPv6 related setting for interfaces. If the interface ID is not specified, all interfaces with the DHCPv6 function will be displayed.

Example

This example shows how to display the DHCPv6 DUID for the device.

```
Switch#show ipv6 dhcp

This device's DUID is 00030006f07d68121001

Switch#
```

This example shows how to display the DHCPv6 setting for interface VLAN 1, when VLAN 1 is DHCPv6 disabled.

```
Switch#show ipv6 dhcp interface vlan1

vlan1 is not in DHCPv6 mode


Switch#
```

This example shows how to display the DHCPv6 setting for all VLANs. Only VLANs that are DHCPv6 enabled are displayed.

```
Switch# show ipv6 dhcp interface

vlan1 is in client mode
  State is OPEN
  List of known servers:
    Reachable via address: FE80::200:11FF:FE22:3344
    Configuration parameters:
        IA PD: IA ID 1, T1 40, T2 64
          Prefix: 2000::/48
                preferred lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```

20. DHCPv6 Guard Commands

20-1 ipv6 dhcp guard policy

This command is used to create or modify a DHCPv6 guard policy, and enter the DHCPv6 Guard Policy Configuration Mode.. Use the **no** form of this command to remove the DHCPv6 guard policy.

ipv6 dhcp guard policy *POLICY-NAME*

no ipv6 dhcp guard policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the DHCPv6 guard policy name.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create or modify the DHCPv6 guard policy, and enter the DHCPv6 Guard Policy Configuration Mode.. DHCPv6 guard policies can be used to block DHCPv6 reply and advertisement messages that come from unauthorized servers. Client messages are not blocked.

After the DHCPv6 guard policy was created, use the **ipv6 dhcp guard attach-policy** command to apply the policy on a specific interface.

Example

This example shows how to create a DHCPv6 guard policy.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)#
```

20-2 device-role

This command is used to specify the role of the attached device. Use the **no** form of this command to revert to the default setting.

device-role {client | server}

no device-role

Parameters

client	Specifies that the attached device is a DHCPv6 client. All DHCPv6 server messages are dropped on this port.
server	Specifies that the attached device is a DHCPv6 server. DHCPv6 server messages are allowed on this port.

Default

By default, this option is **client**.

Command Mode

DHCPv6 Guard Policy Configuration Mode.

Usage Guideline

Use this command to specify the role of the attached device. By default, the device role is client, and all DHCPv6 server messages that came from this port will be dropped. If the device role is set to server, DHCPv6 server messages are allowed on this port.

Example

This example shows how to create a DHCPv6 guard policy and set the device role as the server.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

20-3 match ipv6 access-list

This command is used to verify the sender's IPv6 address in server messages. Use the no form of this command to disable the verification.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*

no match ipv6 access-list

Parameters

IPV6-ACCESS-LIST-NAME	Specifies the IPv6 access list to be matched.

Default

By default, this option is disabled.

Command Mode

DHCPv6 Guard Policy Configuration Mode.

Usage Guideline

Use this command to filter DHCPv6 server message based on sender's IP address. If the **match ipv6 access-list** command is not configured, all server messages are bypassed. An access list is configured by the **ipv6 access-list** command.

Example

This example shows how to create a DHCPv6 guard policy and matches the IPv6 addresses in the access list named list1.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcp_filter1
Switch(config-dhcp-guard)# match ipv6 access-list list1
Switch(config-dhcp-guard)#
```

20-4 ipv6 dhcp guard attach-policy

This command is used to apply a DHCPv6 guard policy on the specified interface. Use the **no** form of this command to remove the binding.

ipv6 dhcp guard attach-policy [*POLICY-NAME***]**

no ipv6 dhcp guard attach-policy

Parameters

POLICY-NAME	(Optional) Specifies the DHCPv6 guard policy name.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to apply a DHCPv6 policy to an interface. DHCPv6 guard policies can be used to block DHCPv6 server messages or filter server messages based on sender IP address. If the policy name is not specified, the default policy will set the device's role to client.

Example

This example shows how to apply the DHCPv6 guard policy "pol1" to port 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

20-5 show ipv6 dhcp guard policy

This command is used to display DHCPv6 guard information.

show ipv6 dhcp guard policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the DHCPv6 guard policy name.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, information of all policies is displayed.

Example

This example shows how to displayed information of all policies.

```
Switch#show ipv6 dhcp guard policy

DHCP guard policy: default
   Device Role: DHCP client
   Target: eth1/0/3

DHCP guard policy: test1
   Device Role: DHCP server
   Source Address Match Access List: acl1
   Target: eth1/0/1

Switch#
```

Display Parameters

Device Role	The role of the device. The role is either client or server.
Target	The name of the target. The target is an interface.
Source Address Match Access List	The IPv6 access list of the specified policy.

21. DHCPv6 Relay Commands

21-1 ipv6 dhcp relay destination

This command is used to enable the DHCP for IPv6 relay service on the interface and specify a destination address to which client messages are forwarded to. Use the **no** form of this command to remove a relay destination.

ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

no ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

Parameters

IPV6-ADDRESS	Specifies the DHCPv6 relay destination address.
INTERFACE-ID	(Optional) Specifies the output interface for the relay destination.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure or remove the relay destination address on an interface. If all relay addresses are removed, the relay function is disabled.

The incoming DHCPv6 messages, being relayed can come from a client, may be already relayed by a relay agent. The destination address to be relayed can be a DHCPv6 server or another DHCPv6 relay agent,

The destination address can be a unicast or a multicast address, both can be a link scoped address or a global scoped address. For link scoped addresses, the interface where the destination address is located must be specified. For global scoped addresses, the user can optional specify the output interface. If the output interface is not specified, the output interface is resolved via the routing table.

Multiple relay destination addresses can be specified for an interface. When the DHCPv6 message is relayed to the multicast address, the hop limit field in the IPv6 packet header will be set to 32.

Example

This example shows how to configure the relay destination address on VLAN 1 and VLAN 2.

```
Switch#configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 dhcp relay destination FE80::250:A2FF:FEBF:A056 vlan1
Switch(config-if)# ipv6 dhcp relay destination FE80::22:33 vlan2
Switch(config-if)#
```

21-2 ipv6 dhcp relay remote-id format

This command is used to configure the sub-type of the remote ID. Use the **no** form of this command to revert to the default settings.

ipv6 dhcp relay remote-id format {default | cid-with-user-define | user-define | expert-udf [standalone_unit_format {0 | 1}]}

no ipv6 dhcp relay remote-id format

Parameters

default

Specifies to use the Switch's system MAC address as the remote ID. The remote ID is formed in the following format:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	MAC Address
1 byte	2 bytes	1 byte	1 byte	6 bytes

F01. Sub Type: The number 1 indicates that this is the remote ID.

F02. VLAN ID: The incoming VLAN ID of the DHCP client packet.

F03. Module ID: For a standalone switch, the module ID is always 0.

F04. Port ID: The incoming port number of the DHCP client packet. The port number starts from 1.

F05. MAC Address: The system MAC address of the Switch.

cid-with-user-define

Specifies to use a CID with user-defined string as the remote ID. The remote ID option is formed in the following format:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	User Defined
1 byte	2 bytes	1 byte	1 byte	Max. 256 bytes

F01. Sub Type: The number 2 indicates that this is the remote ID.

F02. VLAN ID: The incoming VLAN ID of the DHCP client packet.

F03. Module ID: For a standalone switch, the module ID is always 0.

F04. Port ID: The incoming port number of the DHCP client packet. The port number starts from 1.

F05. User Defined: The user-defined string configured in the **ipv6 dhcp relay remote-id udf** command. By default, the field is empty.

user-define

Specifies to use a user-defined string as the remote ID. The remote ID option is formed in the following format:

F01	F02
Sub Type	User Defined
1 byte	Max. 256 bytes

F01. Sub Type: The number 3 indicates that this is the remote ID.

F02. User Defined: The user-defined string configured in the ipv6 dhcp relay remote-id udf command.

expert-udf

Specifies to use a flexible user-defined string as the remote ID. The remote ID option is formed in the following format:

F01
User Defined

	`| Max. 256 bytes |`
	`|----------------|`
	
	F01. User Defined: The flexible user-defined string configured in the **ipv6 dhcp relay remote-id format-type**, **ipv6 dhcp relay remote-id profile**, and **format string** commands. By default, the field is empty.

standalone_unit_format	Specifies the unit ID for the standalone unit. The default value is 0. The parsing rule is defined in the **format string** command.

Default

By default, the format for the DHCPv6 replay remote ID is **default**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the sub-type of the Remote ID option.

Example

This example shows how to configure the sub-type of the remote ID to “cid-with-user-define”.

```
Switch#configure terminal
Switch(config)# ipv6 dhcp relay remote-id format cid-with-user-define
Switch(config)#
```

21-3 ipv6 dhcp relay remote-id option

This command is used to enable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets. Use the **no** form of this command to disable the insert function.

ipv6 dhcp relay remote-id option

no ipv6 dhcp relay remote-id option

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the insertion of the DHCPv6 relay agent Remote ID option function.

Example

This example shows how to enable the insertion of the DHCPv6 relay agent remote ID option.

```
Switch#configure terminal
Switch(config)# ipv6 dhcp relay remote-id option
Switch(config)#
```

21-4 ipv6 dhcp relay remote-id policy

This command is used to configure the Option 37 forwarding policy for the DHCPv6 relay agent. Use the **no** form of this command to revert to the default setting.

ipv6 dhcp relay remote-id policy {drop | keep}

no ipv6 dhcp relay remote-id policy

Parameters

drop	Specifies to discard the packet that already has the relay agent Remote-ID Option 37.
keep	Specifies that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server.

Default

By default, this option is **keep**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the global policy for packets that already have Option 37. If the **drop** parameter is used, relay agent's Remote ID option that has already been presented in the received packet from client, the packet will be dropped. If the **keep** parameter is used, the Switch does not check if there is a relay agent Remote-ID option in the received packet.

Example

This example shows how to configure the policy of the DHCPv6 relay agent Remote ID option to dropping the packet if it has a relay agent Remote-ID option.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

21-5 ipv6 dhcp relay remote-id profile

This command is used to used to create a new profile for DHCPv6 relay Option 37 and enter the DHCPv6 Profile Configuration mode. Use the **no** form of this command to remove the profile.

ipv6 dhcp relay remote-id profile *NAME*

no ipv6 dhcp relay remote-id profile *NAME*

Parameters

NAME	Specifies the profile name. The maximum length is 32 characters. The profile can be created up to 6 entries.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create or remove a profile for DHCPv6 relay Option 37, or enter the DHCPv6 Profile Configuration Mode.

Example

This example shows how to create a profile, profile1, for DHCPv6 relay Option 37.

```
Switch#configure configure terminal
Switch(config)#ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#
```

21-6 format string

This command is used to add a user-defined Option 37. Use the **no** form of this command to delete the entry of the flexible user-defined Option 37.

format string *STRING*

no format string

Parameters

STRING	Specifies the user-defined DHCP Option 37 format with a maximum of 255 characters. The rules that need to follow for this parameters are: • This parameter can be hexadecimal value, ASCII string, or any combination of hexadecimal value and ASCII string. An ASCII string needs to be enclosed with quotation marks (" "), such as "Ethernet"; Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in a packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "%" +"$"+"1-32"+"keyword"+":": **%** - Indicates that the string that follows this character is a formatted key string. **$ or 0** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either “$” or “0”, and cannot be specified as both at the same time. **$** indicates to fill leading space (0x20). **0** indicates to fill leading 0. To fill leading 0 (**0**) is the default setting. **1-32** - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual

length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly.

keyword - Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected:

devtype: The model name of device. Derived from the Module Name field in the show version command. Only an ASCII string is accepted.

sysname: Indicates the System name of the Switch. The maximum length is 128. Only an ASCII string is accepted.

sysname: Indicates the System name of the Switch. Only an ASCII string is accepted.

ifdescr: Derived from ifDescr (IF-MIB). Only an ASCII string is accepted.

portmac: Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of ASCII string, the MAC address format can be customized via special command (e.g., ip dhcp relay information option mac-format case). When in the format of a hexadecimal value, the MAC address will be encapsulated by order in hexadecimal.

sysmac: Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands (e.g., ip dhcp relay information option mac-format case). When in the format of a hexadecimal value, the MAC address will be encapsulated by order in hexadecimal.

module: Indicates the module ID number. This can be either an ASCII string or a hexadecimal value.

port: Indicates the local port number. This can be either an ASCII string or a hexadecimal value.

svlan: Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value.

cvlan: Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value.

: - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (:) can be ignored. The space (0x20) between % and : will be ignored. Other spaces will be encapsulated.

- ASCII strings can be any combination of formatted key strings, 0-9, a-z, A-Z, !, @, #, $, %, ^, &, *, (,), _, +, |, -, =, \, [,], {, }, ;, :, ', ", /, ., ,, <, >, `, and space characters. \ is escape character. The special character after \ is the character itself. For example, \% is % itself, not the start indicator of a formatted key string. Space not in the formatted key string will also be encapsulated.
- Hexadecimal values can be any combination of formatted key strings, 0-9, A-F, a-f, and space characters. The formatted key strings only support keywords which support hexadecimal value. Space not in the formatted key string will be ignored.

Default

None.

Command Mode

DHCPv6 Profile Configuration Mode.

Usage Guideline

Use this command to configure the entry of the flexible user-defined Option 37.

Example

This example shows how to onfigure the entry of the flexible user-defined Option 37.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#format string "%port:\:%sysname:%05svlan"
Switch(config-dhcp-profile)#
```

21-7 ipv6 dhcp relay information option mac-format case

This command is used to define the MAC address format of the DHCPv6 Option 37 flexible user-defined profile. Use the **no** form of this command to revert to the default settings.

ipv6 dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}

no ipv6 dhcp relay information option mac-format case

Parameters

lowercase	Specifies that when using the lowercase format, the Option 37 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff.
uppercase	Specifies that when using uppercase format, the Option 37 MAC address for the user-defined profile username will be formatted as: AA-BB-CC-DD-EE-FF.
hyphen	Specifies that when using “-” as delimiter, the format is: AA-BB-CC-DD-EE-FF.
colon	Specifies that when using “:” as delimiter, the format is: AA:BB:CC:DD:EE:FF.
dot	Specifies that when using “.” as delimiter, the format is: AA.BB.CC.DD.EE.FF.
none	Specifies that when not using any delimiter, the format is: AABBCCDDEEFF.
number	Specifies the delimiter number value. Choose one of the following delimiter options: • **1** - Single delimiter, the format is: AABBCC.DDEEFF. • **2** - Double delimiters, the format is: AABB.CCDD.EEFF. • **5** - Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF. If none is chosen for delimiter, the number does not take effect.

Default

The default authentication MAC address case is **uppercase**.

The default authentication MAC address delimiter is **none**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the MAC address format of the DHCPv6 Option 37 flexible user-defined profile.

Example

This example shows how to specify the MAC address format of the Option 37 flexible user-defined profile.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

21-8 show ipv6 dhcp relay information option mac-format

This command is used to display the MAC address format of the Option 37 profile.

show ipv6 dhcp relay information option mac-format

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the MAC address format of the Option 37 profile.

Example

This example shows how to display the MAC address format of the Option 37 profile.

```
Switch# show ipv6 dhcp relay information option mac-format

 Case              : Uppercase
 Delimiter         : Hyphen
 Delimiter Number  : 5
 Example             : AA-BB-CC-DD-EE-FF

Switch#
```

21-9 ipv6 dhcp relay remote-id udf

This command is used to configure the User Define Field (UDF) for remote ID.

ipv6 dhcp relay remote-id udf {ascii *STRING* **| hex** *HEX-STRING***}**

Parameters

ascii *STRING*	Specifies the ASCII string (a maximum of 128 characters) for the UDF of the Remote ID.
hex *HEX-STRING*	Specifies the hexadecimal string (a maximum of 256 digits) for the UDF of the Remote ID.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the UDF for the Remote ID.

Example

This example shows how to configure the UDF to the ASCII string “PARADISE001”.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf ascii PARADISE001
Switch(config)#
```

This example shows how to configure the UDF to the hexadecimal string “010c08”.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp relay remote-id udf hex 010c08
Switch(config)#
```

21-10 ipv6 dhcp local-relay vlan

This command is used to enable DHCPv6 local relay on a VLAN or a group of VLANs. Use the **no** form of this command to disable the function.

ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**

no ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the DHCPv6 local relay function.

When DHCPv6 local relay is enabled, the Switch will add Option 37 and Option 18 to the request packets from the client.

If the Option 37 check state is enabled, the Switch will check the request packet from the client and drop the packet if it contains Option 37 as specified in the DHCPv6 relay function.

If the Option 37 check state is disabled, the local relay function will always add Option 37 to the request packet, regardless whether the state of Option 37 is enabled or disabled.

The DHCPv6 local relay function will directly forward the packet from the server to the client after which no more processing is done.

Example

This example shows how to enable the DHCPv6 local relay function on VLAN 100.

```
Switch# configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

21-11 show ipv6 dhcp

This command is used to display the DHCPv6 related settings on the interface.

show ipv6 dhcp [interface [*INTERFACE-ID***]]**

Parameters

INTERFACE-ID	(Optional) Specifies the VLAN interface to display the DHCPv6 related settings.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use the **show ipv6 dhcp** command to display the device's DHCPv6 DUID.

Use the **show ipv6 dhcp interface** command to display DHCPv6 related setting for interfaces. If the interface ID is not specified, all interfaces with the DHCPv6 function will be displayed.

Example

This example shows how to display the DHCPv6 settings for VLAN 1, which is in the DHCPv6 relay mode.

```
Switch# show ipv6 dhcp interface vlan1

vlan1 is in relay mode
    Relay destinations:
      FE80::20A:BBFF:FECC:102 via vlan2

Switch #
```

This example shows how to display DHCPv6 information for the interface VLAN 1 when VLAN 1 is not in the DHCPv6 mode.

```
Switch# show ipv6 dhcp interface vlan1

Vlan1 is not in DHCPv6 mode

Switch#
```

21-12 show ipv6 dhcp relay information option

This command is used to display the settings of the DHCPv6 relay information options.

show ipv6 dhcp relay information option

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the settings of the DHCPv6 relay information options.

Example

This example shows how to display the DHCPv6 relay remote ID setting.

```
Switch# show ipv6 dhcp relay information option

IPv6 DHCP relay remote-id
 Policy : drop
 Format : user-define
 UDF is ascii string “userstring”

Switch#
```

21-13 show ipv6 dhcp relay remote-id profile

This command is used to display Option 37 profiles.

show ipv6 dhcp relay remote-id profile

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display Option 37 profiles.

Example

This example shows how to display Option 37 profiles.

```
Switch# show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"


Total Entries:1

Switch#
```

21-14 show ipv6 dhcp relay information option format-type

This command is used to display the format type of the DHCPv6 relay information options.

show ipv6 dhcp relay information option format-type [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the format type of the DHCPv6 relay information options.

Example

This example shows how to display the format type of the DHCPv6 relay information options.

```
Switch# show ipv6 dhcp relay information option format-type

 eth1/0/1
 Remote ID bind profile: 1

 Total Entries: 1
Switch#
```

22. D-Link Discovery Protocol (DDP) Client Commands

22-1 ddp

This command is used to enable DDP client function globally or on the specified interfaces. Use the **no** form of this command to disable DDP client.

ddp

no ddp

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable DDP client function globally or per interface-based.

When DDP is disabled on an interface, the interface will neither process nor generate DDP message. DDP messages received by the interface are flooded in VLAN.

Example

This example shows how to enable DDP globally.

```
Switch# configure terminal
Switch(config)# ddp
Switch(config)#
```

This example shows how to enable DDP on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ddp
Switch(config-if)#
```

22-2 ddp report-timer

This command is used to configure interval between two consecutive DDP report messages. Use the **no** form of this command to revert to the default setting.

ddp report-timer {30 | 60 | 90 | 120 | Never}

no ddp report-timer

Parameters

30	Specifies the report interval to 30 seconds.
60	Specifies the report interval to 60 seconds.
90	Specifies the report interval to 90 seconds.
120	Specifies the report interval to 120 seconds.
Never	Specifies to stop sending report message.

Default

By default, this option is **Never**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure interval between two consecutive DDP report messages.

Example

This example shows how to configure interval to 60 seconds.

```
Switch# configure terminal
Switch(config)# ddp report-timer 60
Switch(config)#
```

22-3 show ddp

This command is used to display the switch DDP configurations.

show ddp [interfaces *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the DDP information of the Switch.

Example

This example shows how to display DDP global information.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
DDP Version:  5
Report timer: Never

Switch#
```

This example shows how to display DDP on port 1.

```
Switch#show ddp interfaces eth1/0/1

Interface         State
--------------    ----------
eth1/0/1          Enabled

Switch#
```

22-4 show ddp neighbors

This command is used to display the information of DDP neighbors.

show ddp neighbors [interface *INTERFACE-ID* **[, | -]] [detail]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
detail	(Optional) Specifies to display the information in detail.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the information of DDP neighbors.

Example

This example shows how to display the information of DDP neighbors.

```
Switch#show ddp neighbors
Total Entries: 2

Interface MAC Address       IP Address                              Product  DDP
                                                                    Category Ver
--------- ----------------- --------------------------------------- -------- ---
eth1/0/8  28-3B-82-7F-5A-08 10.90.90.90                             Switch   5
eth1/0/10 28-3B-82-AA-BB-CC 3FFE:22:33:44::55                       Switch   5

Switch#
```

Display Parameters

Interface	The interface on which the entry was received and learned.
MAC Address	The MAC address of the device.
IP Address	The IPv4/IPv6 address of the device.
Product Category	Identify the product type. **Switch** **AP**: Access point. **NC:** Network camera **VE:** Video encoder **NVR:** Network video recorder **NAS:** Network attached storage **SR:** Service router **WC:** Wireless controller **WS:** Wireless switch **WR:** Wireless router **EPOS**** **AAA-S:** AAA policy server **DS:** Digital signage **NP:** Network printer **CNTRLER:** Controller
DDP Ver	The DDP procotol version.

This example shows how to display the detail information of the DDP neighbor on port 8.

```
Switch#show ddp neighbors interface eth1/0/8 detail
Total Entries: 1

Interface: eth1/0/8
  MAC Address: 28-3B-82-7F-5A-08
  IP Address: 10.90.90.90
  Prefix Length: 24
  Model Name: DGS-3130-54TS
  DDP Version: 5
  Role: Client
  System Name: Switch-East1
  Product Category: Switch
  Firmware Version: 1.10.B024
  Hardware Version: A1
  Serial Number: DDLN7160002

Switch#
```

Display Parameters

Interface	The interface on which the entry was received and learned.
MAC Address	The MAC address of the device.
IP Address	The IPv4/IPv6 address of the device.
Prefix Length	The prefix length.
Model Name	The model name of the device.
DDP Version	The DDP procotol version.
Role	The role of the DDP neighbor. This can be server or client. When the role is server or V2 client, only **Interface**, **MAC Address**, **IP Address**, **DDP Version**, and **Role** are displayed.
System Name	The name of the system.
Product Category	The product type that is carried in the DDP message.
Firmware Version	The firmware version of the device.
Hardware Version	The hardware version of the device.
Serial Number	The serial number of the device.

23. Domain Name System (DNS) Commands

23-1 clear host

This command is used to clear the dynamically learned host entries in the privileged user mode.

clear host {all | [*HOST-NAME*]}

Parameters

all	Specifies to clear all host entries.
HOST-NAME	(Optional) Specifies to delete the specified dynamically learned host entry.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to delete a host entry or all host entries which are dynamically learned by the DNS resolver or caching server.

Example

This example shows how to delete the dynamically entry “www.abc.com” from the host table.

```
Switch# clear host www.abc.com
Switch#
```

23-2 ip domain lookup

This command is used to enable the DNS to carry out the domain name resolution. Use the **no** form of this command to disable the DNS domain name resolution function.

ip domain lookup

no ip domain lookup

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the domain name resolution function. The DNS resolver sends the query to the configured name server. The answer replied by the name server will be cached for answering the subsequent requests.

Example

This example shows how to enable the DNS domain name resolution function.

```
Switch# configure terminal
Switch(config)# ip domain lookup
Switch(config)#
```

23-3 ip host

This command is used to configure the static mapping entry for the host name and the IP address in the host table. Use the **no** form of this command to remove the static host entry.

ip host *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

no ip host *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Parameters

HOST-NAME	Specifies the host name of the equipment.
IP-ADDRESS	Specifies the IPv4 address of the equipment.
IPV6-ADDRESS	Specifies the IPv6 address of the equipment.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The host name specified in this command needs to be qualified.

Example

This example shows how to configure the mapping of the host name “www.abc.com” and the IP address 192.168.5.243.

```
Switch# configure terminal
Switch(config)# ip host www.abc.com 192.168.5.243
Switch(config)#
```

23-4 ip name-server

This command is used to configure the IP address for a domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

no ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

Parameters

IP-ADDRESS	Specifies the IPv4 address for the domain name server.
IPV6-ADDRESS	Specifies the IPv6 address for the domain name server.
IP-ADDRESS2	Specifies a second IPv4 address for the domain name server.
IPV6-ADDRESS2	Specifies a second IPv6 address for the domain name server.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure a DNS server. When the system cannot obtain an answer from a DNS server, it will attempt the subsequent server until it receives a response. If name servers are already configured, the servers configured later will be added to the server list. Two IPv4/IPv6 name servers can be specified.

Example

This example shows how to configure the domain name server 192.168.5.134 and 5001:5::2.

```
Switch# configure terminal
Switch(config)# ip name-server 192.168.5.134 5001:5::2
Switch(config)#
```

23-5 ip name-server timeout

This command is used to configure the timeout value for the name server. Use the **no** form of this command to revert to the default setting.

ip name-server timeout *SECONDS*

no ip name-server timeout

Parameters

SECONDS	Specifies the maximum time to wait for a response from a specified name server. This value must be between 1 and 60.

Default

By default, this value is 3 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the DNS maximum time value to wait for a response from a specified name server.

Example

This example shows how to configure the timeout value to 5 seconds.

```
Switch# configure terminal
Switch(config)# ip name-server timeout 5
Switch(config)#
```

23-6 show hosts

This command is used to display the DNS configuration.

show hosts

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display DNS related configuration information.

Example

This example shows how to display DNS related configuration information.

```
Switch#show hosts

 Number of Static Entries:   1
 Number of Dynamic Entries:  0

 Host Name:          www.abc.com
 IP Address:         192.168.5.243
 Age:                forever


Switch#
```

23-7 show ip name-server

This command is used to display the DNS configuration.

show ip name-server

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the DNS related configuration information.

Example

This example shows how to display the DNS related configuration information.

```
Switch# show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

Switch#
```

24. DoS Prevention Commands

24-1 dos-prevention

This command is used to enable and configure the DoS prevention mechanism. Use the **no** form of this command to reset DoS prevention to the default setting.

dos-prevention *DOS-ATTACK-TYPE*

no dos-prevention *DOS-ATTACK-TYPE*

Parameters

DOS-ATTACK-TYPE	Specifies the string that identifies the DoS type to be configured.

Default

By default all supported DoS types are disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use the **dos-prevention** *DOS-ATTACK-TYPE* command to enabled and configure the DoS prevention mechanism for a specific DoS attack type or for all supported types. The DoS prevention mechanisms (matching and taking action) are hardware-based features.

When DoS prevention is enabled, the Switch will log the event if any attack packet was received.

Use the no **dos-prevention all** command to disable the DoS prevention mechanism for all supported types. All the related settings will be reverted back to the default for the specified attack types.

The following well-known DoS types which can be detected by most switches:

- **Blat** - This type of attack will send packets with TCP/UDP source port equals to destination port to the target device. It may cause the target device respond to itself.
- **Land** - A LAND attack involves with IP packets where the source and destination address are set to address of the target device. It may cause the target device reply to itself continuously.
- **TCP-NULL-scan**: Port scanning by using specific packets, which contain a sequence number of 0 and no flags.
- **TCP-SYN-fin** - Port scanning by using specific packets, which contain SYN and FIN flags.
- **TCP-SYN-SRCport-less-1024**: Port scanning by using specific packets, which contain source port 0-1023 and SYN flag.
- **TCP-xmas-scan** - Port scanning by using specific packets, which contain a sequence number of 0 and the Urgent (URG), Push (PSH), and FIN flags.
- **Ping-death** - A ping of death is a type of attack on a computer that involves sending a malformed or otherwise malicious ping to a computer. A ping is normally 64 bytes in size; many computers cannot handle a ping larger than the maximum IP packet size, which is 65,535 bytes. Sending a ping of this size can crash the target computer. Traditionally, this bug has been relatively easy to exploit. Generally, sending a 65536 byte ping packet is illegal according to networking protocol, but a packet of such a size can be sent if it is fragmented; when the target computer reassembles the packet, a buffer overflow can occur, which often cause a system crash.
- **TCP-tiny-frag** - Tiny TCP Fragment attacker uses the IP fragmentation to create extremely small fragments and force the TCP header information into a separate packet fragment to pass through the check function of the router and issue an attack.
- **All** - All of above types.

Example

This example shows how to enable the DoS prevention mechanism for land attack.

```
Switch# configure terminal
Switch(config)# dos-prevention land
Switch(config)#
```

This example shows how to enable the DoS prevention mechanism on all supported types.

```
Switch# configure terminal
Switch(config)# no dos-prevention all
Switch(config)#
```

This example shows how to disable the DoS prevention mechanism for all supported types.

```
Switch# configure terminal
Switch(config)# dos-prevention all
Switch(config)#
```

24-2 show dos-prevention

This command is used to display the DoS prevention status.

show dos-prevention [*DOS-ATTACK-TYPE***]**

Parameters

DOS-ATTACK-TYPE	(Optional) Specifies the DoS type to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about DoS prevention.

Example

This example shows how to display the configuration information of the DoS prevention.

```
Switch#show dos-prevention

DoS Prevention Information
DoS Type                     State
------------------------- --------
Land Attack                Disabled
Blat Attack                Disabled
TCP Null                   Disabled
TCP Xmas                   Disabled
TCP SYN-FIN                Disabled
TCP SYN SrcPort Less 1024  Disabled
Ping of Death Attack       Disabled
TCP Tiny Fragment Attack   Disabled

Switch#
```

This example shows how to display the specified type configuration information of the DoS prevention.

```
Switch# show dos-prevention land

DoS Type    : Land Attack
State        : Enabled

Switch#
```

24-3 snmp-server enable traps dos-prevention

This command is used to enable the sending of SNMP notifications for DoS attacking. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps dos-prevention

no snmp-server enable traps dos-prevention

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

When DoS prevention is enabled, every five minutes, the Switch will log the event if any attack packet is received in this interval. Use this command to enable or disable the sending of SNMP notifications for such events.

Example

This example shows how to enable the sending of traps for DoS attacking.

```
Switch# onfigure terminal
Switch(config)# snmp-server enable traps dos-prevention
Switch(config)#
```

25. Dynamic ARP Inspection Commands

25-1 arp access-list

This command is used to create or modify an ARP access list. This command will enter into the ARP access-list configuration mode. Use the **no** form of this command to remove an ARP access-list.

arp access-list *NAME*

no arp access-list *NAME*

Parameters

NAME	Specifies the name of the ARP access-list to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The name must be unique among all access-lists. The characters used in the name are case sensitive. There is an implicit deny statement at the end of an access list.

Example

This example shows how to configure an ARP access list with two permit entries.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

25-2 clear ip arp inspection log

This command is used to clear the ARP inspection log buffer.

clear ip arp inspection log

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the ARP inspection log buffer.

Example

This example shows how to clear the inspection log.

```
Switch# clear ip arp inspection log
Switch#
```

25-3 clear ip arp inspection statistics

This command is used to clear the dynamic ARP inspection statistics.

clear ip arp inspection statistics {all | vlan *VLAN-ID* **[, | -]}**

Parameters

all	Specifies to clear dynamic ARP inspection statistics from all VLANs.
vlan *VLAN-ID*	Specifies the VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the Dynamic ARP Inspection (DAI) statistics.

Example

This example shows how to clear the DAI statistics from VLAN 1.

```
Switch#clear ip arp inspection statistics vlan 1
Switch#
```

25-4 ip arp inspection filter vlan

This command is used to specify an ARP access list to be used for ARP inspection checks for the VLAN. Use the **no** form of this command to remove the specification.

ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

no ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

Parameters

ARP-ACL-NAME	Specifies the access control list name with a maximum of 32 characters.
vlan *VLAN-ID*	Specifies the VLAN associated with the ARP access list.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
static	(Optional) Specifies to drop the packet if the IP-to-Ethernet MAC binding pair is not permitted by the ARP ACL.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify an ARP access list to be used for ARP inspection checks for the VLAN. Up to one access list can be specified for a VLAN.

The dynamic ARP inspection checks the ARP packets received on the VLAN to verify that the binding pair of the source IP and source MAC address of the packet is valid. The validation process will match the address binging against the entries of the DHCP snooping database. If the command is configured, the validation process will match the address binging against the access list entries and the DHCP snooping database.

ARP ACLs take precedence over entries in the DHCP snooping binding database. If the packet is explicitly denied by the access control list, the packet is dropped. If the packet is denied due to the implicit deny and the **static** parameter is not specified, the packet will be further matched against the DHCP snooping binding entries. If the packet is denied due to the implicit deny and the **static** parameter is specified, the packet will be dropped.

Example

This example shows how to apply the ARP ACL static ARP list to VLAN 10 for DAI.

```
Switch# configure terminal
Switch(config)# ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

25-5 ip arp inspection limit

This command is used to limit the rate of incoming ARP requests and responses on an interface. Use the **no** form of this command to revert to the default settings.

ip arp inspection limit {rate *VALUE* **[burst interval** *SECONDS***] | none}**

no ip arp inspection limit

Parameters

rate *VALUE*	Specifies the maximum number of the ARP packets that can be processed. The valid range is from 1 to 150 seconds.
burst interval *SECONDS*	(Optional) Specifies the length of the burst duration of the ARP packets that is allowed. The valid range is from 1 to 15. If not specified, the default setting is one second.

none	Specifies that there is no limit on the ARP packet rate.

Default

For DAI untrusted interfaces, the rate limit is 15 packets per second with a burst interval of 1 second.

For DAI trusted interfaces, the rate has no limit.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

This command takes effect for both trusted and un-trusted interfaces. When the rate of the ARP packet per second exceeds the limitation and the condition sustained for the configured burst duration, the port will be put in the error disable state.

Example

This example shows how to limit the rate of the incoming ARP requests to 30 packets per second and to set the interface monitoring interval to 5 consecutive seconds.

```
Switch# configure terminal
Switch(config)# interface eth1/0/10
Switch(config-if)# ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

25-6 ip arp inspection log-buffer

This command is used to configure the ARP inspection log buffer parameter. Use the **no** form of this command to revert to the default setting.

ip arp inspection log-buffer entries *NUMBER*

no ip arp inspection log-buffer entries

Parameters

NUMBER	Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the maximum entry number of the log buffer. The ARP inspection log buffer keeps tracks the information of ARP packet. The first packet that is given by check will be sent to syslog module and recorded in the inspection log buffer. The subsequent packets belonging to the same session will not be sent to log module unless its record in the log buffer is cleared. If the log buffer is full but more logging events, the event will not be logged. If the user specifies a buffer size less than the current entry number, the log buffer will be automatically cleared.

Example

This example shows how to change the maximum buffer number to 64.

```
Switch# configure terminal
Switch(config)# ip arp inspection log-buffer entries 64
Switch(config)#
```

25-7 ip arp inspection trust

This command is used to configure an interface for dynamic ARP inspection in the trusted state. Use the **no** form of this command to configure the interface in the untrusted state.

ip arp inspection trust

no ip arp inspection trust

Parameters

None.

Default

By default, the untrusted state is used.

Command Mode

Interface Configuration Mode.

Usage Guideline

When an interface is in the trusted state, the ARP packets arriving at the interface will not be inspected. When an interface is in the untrusted state, ARP packets arriving at the port and belongs to the VLAN that is enabled for inspection will be inspected.

Example

This example shows how to configure port 3 to be trusted for DAI.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)#
```

25-8 ip arp inspection validate

This command is used to specify the additional checks to be performed during an ARP inspection check. Use the **no** form of this command to remove specific additional check.

ip arp inspection validate [src-mac] [dst-mac] [ip]

no ip arp inspection validate [src-mac] [dst-mac] [ip]

Parameters

src-mac	(Optional) Specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.

dst-mac	(Optional) Specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
ip	(Optional) Specifies to check the ARP body for invalid and unexpected IP addresses. Specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the additional checks to be performed during the dynamic ARP inspection check. The specified check will be performed on packets arriving at the untrusted interface and belong to the VLANs that are enabled for IP ARP inspection. If no parameter is specified, all options are enabled or disabled.

Example

This example shows how to enable source MAC validation.

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)#
```

25-9 ip arp inspection vlan

This command is used to enable specific VLANs for dynamic ARP inspection. Use the **no** form of this command to disable dynamic ARP inspection for VLAN.

ip arp inspection vlan *VLAN-ID* **[, | -]**

no ip arp inspection vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the VLAN to enable or disable the ARP inspection function.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, ARP inspection is disabled on all VLANs.

Command Mode

Global Configuration Mode.

Usage Guideline

When a VLAN is enabled for ARP inspection, the ARP packets, including both the ARP request and response packet belonging to the VLAN arriving at the untrusted interface will be validated. If the IP-to-MAC address binding pair of the source MAC address and the source IP address is not permitted by the ARP ACL or the DHCP snooping binding database, the ARP packet will be dropped. In addition to the address binding check, the additional check defined by the IP ARP inspection validate command will also be checked.

Example

This example shows how to enable ARP inspection on VLAN 2.

```
Switch#configure terminal
Switch(config)# ip arp inspection vlan 2
Switch(config)#
```

25-10 ip arp inspection vlan logging

This command is used to control the type of packets that are logged. Use the **no** form of this command to revert to the default settings.

ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match {permit | all | none} | dhcp-bindings {permit | all | none}}**

no ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match | dhcp-bindings}**

Parameters

VLAN-ID	Specifies the VLAN to enable or disable the logging control function.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
acl-match permit	Specifies logging when permitted by the configured ACL.
acl-match all	Specifies logging when permitted or denied by the configured ACL.
acl-match none	Specifies that ACL-matched packets are not logged.
dhcp-bindings	Specifies the logging criteria for packets dropped or permitted based on matches against the DHCP bindings.
dhcp-bindings permit	Specifies logging when permitted by DHCP bindings.
dhcp-bindings all	Specifies logging when permitted or denied by DHCP bindings.
dhcp-bindings none	Specifies to prevent the logging of all packets permitted or denied by DHCP bindings.

Default

By default, **acl-match** and **dhcp-bindings** log denied packets.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the logging criteria for packets. When using the **no** command, the **acl-match** and **dhcp-bindings** parameters are reverted to the default setting individually.

Example

This example shows how to configure an ARP inspection on VLAN 1 to add packets to a log that matches the ACLs.

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1 logging acl-match all
Switch(config)#
```

25-11 permit | deny (arp access-list)

This command is used to add a permit or deny ARP entry. Use the **no** form of this command to remove an entry.

{permit | deny} ip {any | host *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

no {permit | deny} ip {any | host *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

Parameters

ip any	Specifies to match any source IP address.
ip host *SENDER-IP*	Specifies to match a single source IP address.
SENDER-IP SENDER-IP-MASK	Specifies to match a group of source IP addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as IP address.
mac any	Specifies to match any source MAC address.
mac host *SENDER-MAC*	Specifies to match a single source MAC address.
SENDER-MAC SENDER-MAC-MASK	Specifies to match a group of source MAC addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as MAC address.

Default

None.

Command Mode

ARP Access-list Configuration Mode.

Usage Guideline

Using the **permit any** option will permit the rest of the packets that do not match any previous rule.

Example

This example shows how to configure an ARP access-list with two permit entries.

```
Switch# configure terminal
Switch(config)# arp access-list static-arp-list
Switch(config-arp-nacl)# permit ip 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

25-12 show ip arp inspection

This command is used to display the status of DAI for a specific range of VLANs.

show ip arp inspection [interfaces [*INTERFACE-ID* **[, | -]] | statistics [vlan** *VLAN-ID* **[, | -]]]**

Parameters

interfaces	(Optional) Specifies a port or range of ports.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
statistics	(Optional) Specifies the DAI statistics.
vlan *VLAN-ID*	(Optional) Specifies a VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the status of DAI for a specific range of VLANs.

Example

This example shows how to display the statistics of packets that have been processed by DAI for VLAN 10.

```
Switch#show ip arp inspection statistics vlan 10

VLAN Forwarded Dropped  DHCP Drops ACL Drops
---- --------- --------- --------- ---------
10   21546     145261    145261    0
VLAN DHCP Permits ACL Permits  Source MAC Failures
---- ------------ ------------ -------------------
10   21546        0            0
VLAN Dest MAC Failures IP Validation Failures
---- ----------------- ----------------------
10   0                 0

Switch#
```

This example shows how to display the statistics of packets that have been processed by DAI for all active VLANs.

```
Switch#show ip arp inspection statistics

VLAN Forwarded Dropped  DHCP Drops ACL Drops
---- --------- --------- --------- ---------
1    0         0         0         0
2    0         0         0         0
10   21546     145261    145261    0
100  0         0         0         0
200  0         0         0         0
1024 0         0         0         0
VLAN DHCP Permits ACL Permits  Source MAC Failures
---- ------------ ------------ -------------------
1    0            0            0
2    0            0            0
10   21546        0            0
100  0            0            0
200  0            0            0
1024 0            0            0
VLAN Dest MAC Failures IP Validation Failures
---- ----------------- ----------------------
1    0                 0
2    0                 0
10   0                 0
100  0                 0
200  0                 0
1024 0                 0

Switch#
```

Display Parameters

VLAN	The VLAN ID that is enabled for ARP inspection.
Forwarded	The number of ARP packets that are forwarded by ARP inspection.
Dropped	The number of ARP packets that are dropped by ARP inspection.
DHCP Drops	The number of ARP packets that are dropped by DHCP snooping binding database.

ACL Drops	The number of ARP packets that are dropped by ARP ACL rule.
DHCP Permits	The number of ARP packets that are permitted by DHCP snooping binding database.
ACL Permits	The number of ARP packets that are permitted by ARP ACL rule.
Source MAC Failures	The number of ARP packets that fail source MAC validation.
Dest MAC Failures	The number of ARP packets that fail destination MAC validation.
IP Validation Failures	The number of ARP packets that fail the IP address validation.

This example shows how to display the configuration and operating state of DAI.

```
Switch#show ip arp inspection

Source MAC Validation     : Disabled
Destination MAC Validation: Disabled
IP Address Validation     : Disabled
VLAN State    ACL Match                         Static ACL
---- -------- --------------------------------- ----------
2    Enabled  -                                 -
VLAN ACL Logging DHCP Logging
---- ----------- ------------
2    None        None

Switch#
```

Display Parameters

VLAN	The VLAN ID that is enabled for ARP inspection.
Configuration	The configuration state of ARP inspection. • **Enable** - ARP inspection is enabled. • **Disable** - ARP inspection is enabled.
ACL Match	The name of ARP ACL that is specified.
Static ACL	The configuration of the static ACL. • **Yes** - Static ARP ACL is configured. • **No** - Static ARP ACL is not configured.
ACL logging	The state of logging for packets dropped or permitted based on ACL matches. • **None** - ACL-matched packets are not logged. • **Permit** - Logging when packets are permitted by the configured ACL. • **Deny** - Logging when packets are dropped by the configured ACL. • **All** - ACL-matched packets are always logged.
DHCP Logging	The state of logging for packets dropped or permitted based on DHCP bindings. • **None** - Prevent logging when packets are dropped or permitted by the DHCP bindings. • **Permit** - Logging when packets are permitted by the DHCP bindings. • **Deny** - Logging when packets are dropped by the DHCP bindings. • **All** - Logging when packets are dropped or permitted by the DHCP bindings.

This example shows how to display the trust state of port 3.

```
Switch#show ip arp inspection interfaces eth1/0/3

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/3        untrusted   15        1
Total Entries: 1

Switch#
```

This example shows how to display the trust state of interfaces on the Switch.

```
Switch#show ip arp inspection interfaces eth1/0/1-7

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/1        untrusted   15        1
eth1/0/2        untrusted   15        1
eth1/0/3        untrusted   15        1
eth1/0/4        untrusted   15        1
eth1/0/5        untrusted   15        1
eth1/0/6        untrusted   15        1
eth1/0/7        untrusted   15        1
Total Entries: 7

Switch#
```

Display Parameters

Interface	The name of interface that enable ARP inspection.
Trust State	The state of the interface. • **trusted** - This interface is ARP inspection trusted port, all ARP packet will be legal and not be authorized. • **untrusted** - This interface is ARP inspection untrusted port, all ARP packet will be authorized.
Rate (pps)	The upper limit on the number of incoming packets processed per second.
Burst Interval	The consecutive interval in seconds over which the interface is monitored for the high rate of the ARP packets.

25-13 show ip arp inspection log

This command is used to display the ARP inspection log buffer.

show ip arp inspection log

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the content of the inspection log buffer.

Example

This example shows how to display the inspection log-buffer.

```
Switch#show ip arp inspection log
Total log buffer size: 32

Interface       VLAN Sender IP       Sender MAC        Occurrence
--------------- ---- --------------- ----------------- ------------------------
eth1/0/1        100  10.20.1.1       00-20-30-40-50-60 1 (2014-03-28 23:08:66)
eth1/0/2        100  10.5.10.16      55-66-20-30-40-50 2 (2014-04-02 00:11:54)
eth1/0/3        100  10.58.2.30      10-22-33-44-50-60 1 (2014-03-30 12:01:38)

Total Entries: 3

Switch#
```

Display Parameters

Interface	The name of interface that logging occurred.
VLAN	The VLAN that logging occurred.
Sender IP	The logging ARP’s sender IP address.
Sender MAC	The logging ARP’s sender MAC address.
Occurrence	The counter of logging entries occurred and the last time of logging entry occurred.

26. Error Recovery Commands

26-1 errdisable recovery

This command is used to enable the error recovery for causes and to configure the recovery interval. Use the **no** form of this command to disable the auto-recovery option or to return interval to the default setting for causes.

errdisable recovery cause {all | psecure-violation | storm-control | arp-rate | dhcp-rate | loopback-detect} [interval *SECONDS***]**

no errdisable recovery cause {all | psecure-violation | storm-control | arp-rate | dhcp-rate | loopback-detect} [interval]

Parameters

all	Specifies to enable the auto-recovery option for all causes.
psecure-violation	Specifies to enable the auto-recovery option for an error port caused by port security violation.
storm-control	Specifies to enable the auto-recovery option for an error port caused by storm control.
arp-rate	Specifies to enable the auto-recovery option for an error port caused by ARP rate limiting.
dhcp-rate	Specifies to enable the auto-recovery option for an error port caused by DHCP rate limiting.
loopback-detect	Specifies to enable the auto-recovery option for an error port caused by loop detection.
interval *SECONDS*	Specifies the time in seconds to recover the port from the error state caused by the specified module. The valid value is 5 to 86400. The default value is 300 seconds.

Default

Auto recovery is disabled for all causes.

Command Mode

Global Configuration Mode.

Usage Guideline

A port can be put in an error disabled state by causes such as port security violations, storm control, and so on. When a port enters the error disabled state, the port is shutdown although the setting running the configuration remains in the no shutdown state.

There are two ways to recover an error disabled port. Administrators can use the **errdisable recovery cause** command to enable the auto-recovery of error ports disabled by each cause. Alternatively, administrators can manually recover the port by entering the **shutdown** command first and then the **no shutdown** command for the port.

Example

This example shows how to set the recovery timer to 200 seconds for port security violation.

```
Switch# configure terminal
Switch(config)# errdisable recovery cause psecure-violation interval 200
Switch(config)#
```

This example shows how to enable the auto-recovery option for port security violations.

```
Switch# configure terminal
Switch(config)# errdisable recovery cause psecure-violation
Switch(config)#
```

26-2 show errdisable recovery

This command is used to display the error-disable recovery timer related settings.

show errdisable recovery

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to verify the settings of the error disable recovery timer.

Example

This example shows how to display the settings of the error disable recovery timer.

```
Switch# show errdisable recovery

ErrDisable Cause                        State         Interval
--------------------------------------  -----------   -------------
Port Security                           enabled       200 seconds
Storm Control                           disabled      300 seconds
Dynamic ARP Inspection                  disabled      300 seconds
DHCP Snooping                           disabled      300 seconds
Loop Detection                          disabled      300 seconds

Interfaces that will be recovered at the next timeout:

Switch#
```

26-3 snmp-server enable traps errdisable

This command is used to enable the sending of SNMP notifications for the error disabled state. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps errdisable [asserted] [cleared] [notification-rate *TRAP-RATE***]**

no snmp-server enable traps errdisable [asserted] [cleared] [notification-rate]

Parameters

asserted	(Optional) Specifies to control the notifications when entering into the error disabled state.
cleared	(Optional) Specifies to control the notifications when exiting from the error disabled state.
notification-rate *TRAP-RATE*	(Optional) Specifies the number of traps per minute. The value is from 0 to 1000. If the number of packets exceeds the specified number, the exceeded packets will be dropped. 0 represents that there is no limitation for the sending of the SNMP traps for the error disabled state per minute.

Default

By default, this feature is disabled.

By default, the notification rate is 0.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command with the **asserted** and **cleared** parameters to enable or disable the notifications for the state change of the error disabled state. If one of the parameters is specified, only the specified notification type is enabled or disabled. The state or value of the other notification type will not be affected.

The **snmp-server enable traps errdisable notification-rate** and **no snmp-server enable traps errdisable notification-rate** commands only affect the setting of notification-rate, but not the state of the sending notifications for the error disabled state.

Example

This example shows how to enable the sending of traps for entering into and exiting from the error disabled state and set the maximum number of traps per second to 3.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps errdisable asserted cleared notification-rate 3
Switch(config)#
```

27. File System Commands

27-1 delete

This command is used to delete a file.

delete *FILE-URL*

Parameters

FILE-URL	Specifies the name of the file to be deleted.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

The firmware image or the configuration file that is specified as the boot-up file cannot be deleted.

Example

This example shows how to delete the file named “Image2” from file system on the local flash.

```
Switch#delete Image2
Delete Image2? (y/n) [n]  y
File is deleted.

Switch#
```

27-2 dir

This command is used to display the information for a file or the listing of files in the specified path name.

dir [*URL***]**

Parameters

URL	(Optional) Specifies the name of the file or directory to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, the current directory is used. By default, the current directly is located at the root of the file system located at local flash. The storage media is mounted in the file system and appears to the user as a sub-directory under the root directory.

The supported file systems can be displayed as the user issues the dir command for the root directory. The storage media that is mapped to the file system can be displayed by using the show storage media command.

Example

This example shows how to display the root directory in a standalone switch.

```
Switch#dir

Directory of /c:
1   -rw      21045792 Jan 01 2019 00:04:39  Image1
2   -rw      15720992 Jan 01 2019 00:06:39  Image2
3   -rw          1481 Jan 01 2019 00:02:07  Config1
4   d--             0 Jan 01 2019 00:02:07  system

66191360 bytes total (21315584 bytes free)

Switch#
```

27-3 show storage media-info

This command is used to display the storage media's information.

show storage media-info

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the information of the storage media available on the system.

Example

This example shows how to display the information of the storage media.

```
Switch#show storage media-info

Drive  Media Type  Size      FS-Type  Label
-----  ----------  --------  -------  -----------
c:     Flash       63 MB     swfs

Switch#
```

28. Filter Database (FDB) Commands

28-1 clear mac-address-table

This command is used to delete a specific dynamic MAC address, all dynamic MAC addresses on a particular interface, all dynamic MAC addresses on a particular VLAN, or all dynamic MAC addresses from the MAC address table.

clear mac-address-table dynamic {all | address *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***}**

Parameters

all	Specifies to clear all dynamic MAC addresses.
address *MAC-ADDR*	Specifies to delete the specified dynamic MAC address.
interface *INTERFACE-ID*	Secifies the interface that the MAC address will be deleted from. The specified interface can be a physical port or a port-channel.
vlan *VLAN-ID*	Specifies the VLAN ID. The valid values are from 1 to 4094.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to only clear dynamic MAC address entries. Only the dynamic unicast address entry will be cleared.

Example

This example shows how to remove the MAC address 00:08:00:70:00:07 from the dynamic MAC address table.

```
Switch# clear mac-address-table dynamic address 00:08:00:70:00:07
Switch#
```

28-2 mac-address-table aging-time

This command is used to configure the MAC address table aging time. Use the **no** form of this command to revert to the default setting.

mac-address-table aging-time *SECONDS*

no mac-address-table aging-time

Parameters

SECONDS	Specifies the aging time in seconds. The valid range is 0 or 10 to 1000000 seconds. Setting the aging time to 0 will disable the MAC address table aging out function.

Default

By default, this value is 300 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Setting the aging time to 0 will disable the MAC address table aging out function.

Example

This example shows how to set the aging time value to 200 seconds.

```
Switch# configure terminal
Switch(config)# mac-address-table aging-time 200
Switch(config)#
```

28-3 mac-address-table learning

This command is used to enable MAC address learning on the physical port. Use the **no** form of this command to disable learning.

mac-address-table learning interface *INTERFACE-ID* **[, | -]**

no mac-address-table learning interface *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the interfaces to be configured.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to enable or disable MAC address learning on a physical port.

Example

This example shows how to enable the MAC address learning option.

```
Switch# configure terminal
Switch(config)# mac-address-table learning interface eth1/0/5
Switch(config)#
```

28-4 mac-address-table notification change

This command is used to enable or configure the MAC address notification function. Use the **no** form of this command to disable the function or revert the optional configuration to default.

mac-address-table notification change [interval *SECONDS* **| history-size** *VALUE* **| trap-type {with-vlanid | without-vlanid}]**

no mac-address-table notification change [interval | history-size | trap-type]

Parameters

interval *SECONDS*	(Optional) Specifies the interval of sending the MAC address trap message. The range is 1 to 2147483647 and the default value is 1 second.
history-size *VALUE*	(Optional) Specifies the maximum number of the entries in the MAC history notification table. The range is 0 to 500 and the default value is 1 entry.
trap-type	(Optional) Specifies the trap information to include VLAN ID or not.
with-vlanid	Specifies the trap information to include VLAN ID.
without-vlanid	Specifies the trap information to exclude VLAN ID.

Default

MAC address notification is disabled.

The default trap interval is 1 second.

The default number of entries in the history table is 1.

The default trap type is without-vlanid.

Command Mode

Global Configuration Mode.

Usage Guideline

When the Switch learns or removes a MAC address, a notification can be sent to the notification history table and then sent to the SNMP server if the **snmp-server enable traps mac-notification change** command is enabled. The MAC notification history table stores the MAC address learned or deleted on each interface for which the trap is enabled. Events are not generated for multicast addresses.

Example

This example shows how to enable MAC address change notification and set the interval to 10 seconds and set the history size value to 500 entries.

```
Switch# configure terminal
Switch(config)# mac-address-table notification change
Switch(config)# mac-address-table notification change interval 10
Switch(config)# mac-address-table notification change history-size 500
Switch(config)#
```

28-5 mac-address-table static

This command is used to add a static address to the MAC address table. Use the **no** form of this command to remove a static MAC address entry from the table.

mac-address-table static *MAC-ADDR* **vlan** *VLAN-ID* **{interface** *INTERFACE-ID* **[, | -] | drop}**

no mac-address-table static {all | *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID***] [, | -]}**

Parameters

MAC-ADDR	Specifies the MAC address of the entry. The address can be a unicast or a multicast entry. Packets with a destination address that match this MAC address received by the specified VLAN are forwarded to the specified interface.
vlan *VLAN-ID*	Specifies the VLAN of the entry. The range is 1 to 4094.
interface *INTERFACE-ID*	Specifies the forwarding ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
drop	Specifies to drop the frames that are sent by or sent to the specified MAC address on the specified VLAN.
all	Specifies to remove all static MAC address entries.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

For a unicast MAC address entry, only one interface can be specified. For a multicast MAC address entry, multiple interfaces can be specified. To delete a unicast MAC address entry, there is no need to specify the interface ID. To delete a multicast MAC address entry, if an interface ID is specified, only this interface will be removed. Otherwise, the entire multicast MAC entry will be removed. The option drop can only be specified for a unicast MAC address entry.

Example

This example shows how to add the static address C2:F3:22:0A:12:F4 to the MAC address table. It also specifies that when any packet received on VLAN 4 that has a destination MAC address of C2:F3:22:0A:12:F4 will be forwarded to port 1.

```
Switch# configure terminal
Switch(config)# mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface eth1/0/1
Switch(config)#
```

28-6 multicast filtering-mode

This command is used to configure the handling method for multicast packets for a VLAN. Use the **no** form of this command to revert to the default setting.

multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}

no multicast filtering-mode

Parameters

forward-all	Specifies to flood all multicast packets based on the VLAN domain.
forward-unregistered	Specifies to forward registered multicast packets based on the forwarding table and flood all unregistered multicast packets based on the VLAN domain.
filter-unregistered	Specifies to forward registered packets based on the forwarding table and filter all unregistered multicast packets.

Default

By default, the forward-unregistered option is enabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

This filtering mode is only applied to multicast packets that are destined for addresses other than those reserved for multicast addresses.

Example

This example shows how to set the multicast filtering mode on VLAN 100 to filter unregistered.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# multicast filtering-mode filter-unregistered
Switch(config-vlan)#
```

28-7 show mac-address-table

This command is used to display a specific MAC address entry or the MAC address entries for a specific interface or VLAN.

show mac-address-table [dynamic | static] [address *MAC-ADDR* **| interface** *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Parameters

dynamic	(Optional) Specifies to display dynamic MAC address table entries only.
static	(Optional) Specifies to display static MAC address table entries only.
address *MAC-ADDR*	(Optional) Specifies the 48-bit MAC address.
interface *INTERFACE-ID*	(Optional) Specifies the interface to be displayed. Only physical port and port-channel interfaces are allowed to be specified.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID. The valid values are from 1 to 4094.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If the **interface** parameter is specified, the unicast entry that has the forwarding interface matches the specified interface will be displayed.

Example

This example shows how to display all the MAC address table entries for the MAC address 00-02-4b-28-c4-82.

```
Switch# show mac-address-table address 00:02:4B:28:C4:82

VLAN    MAC Address        Type    Ports
------ ----------------- -------- --------
1      00-02-4B-28-C4-82   Static   CPU

Total Entries: 1

Switch#
```

This example shows how to display all the static MAC address table entries.

```
Switch# show mac-address-table static
VLAN    MAC Address          Type     Ports
----------------------------------------
1     00-02-4B-28-C4-82     Static    CPU
2     00-02-4B-28-C4-82     Static    CPU
4     00-01-00-02-00-04     Static    eth1/0/2
4     C2-F3-22-0A-12-F4     Static    port-channel2
6     00-01-00-02-00-07     Static    eth1/0/1
6     00-01-00-02-00-10     Static    Drop

Total Entries : 6

Switch#
```

This example shows how to display all the MAC address table entries for VLAN 1.

```
Switch# show mac-address-table vlan 1

VLAN   MAC Address          Type         Ports
-----------------------------------------------------
1     00-02-4B-28-C4-82    Static         CPU
1     00-03-40-11-22-33    Dynamic        eth1/0/2

Total Entries: 2

Switch#
```

28-8 show mac-address-table aging-time

This command is used to display the aging time of the MAC address table.

show mac-address-table aging-time

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the aging time of the MAC address table.

Example

This example shows how to display the aging time of the MAC address table.

```
Switch# show mac-address-table aging-time

Aging Time is 300 seconds

Switch#
```

28-9 show mac-address-table learning

This command is used to display the MAC-address learning state.

show mac-address-table learning [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.

,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all existing interfaces will be displayed.

Example

This example shows how to display the MAC address learning status on ports 1 to 10.

```
Switch#show mac-address-table learning interface eth1/0/1-10

Port                        Status
--------------------------  --------
eth1/0/1                    Enabled
eth1/0/2                    Enabled
eth1/0/3                    Enabled
eth1/0/4                    Enabled
eth1/0/5                    Enabled
eth1/0/6                    Enabled
eth1/0/7                    Enabled
eth1/0/8                    Enabled
eth1/0/9                    Enabled
eth1/0/10                   Enabled

Switch#
```

28-10 show mac-address-table notification change

This command is used to display the MAC address notification configuration or history content.

show mac-address-table notification change [interface [*INTERFACE-ID*] | history]

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
history	(Optional) Specifies to display the MAC address notification change history.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, the global configuration will be displayed. Use the **interface** parameter to display information of all interfaces. Use the **interface** *INTERFACE-ID* parameter to display information of the specified interface.

Example

This example shows how to display the MAC address notification change configuration on all interfaces.

```
Switch# show mac-address-table notification change interface

Interface                Added Trap       Removed Trap
-----------------------  --------------   --------------

eth1/0/1                 Disabled         Disabled
eth1/0/2                 Disabled         Disabled
eth1/0/3                 Disabled         Disabled
eth1/0/4                 Disabled         Disabled
eth1/0/5                 Disabled         Disabled
eth1/0/6                 Disabled         Disabled
eth1/0/7                 Disabled         Disabled
eth1/0/8                 Disabled         Disabled
eth1/0/9                 Disabled         Disabled
eth1/0/10                Disabled         Disabled
eth1/0/11                Disabled         Disabled
eth1/0/12                Disabled         Disabled
eth1/0/13                Disabled         Disabled
eth1/0/14                Disabled         Disabled
eth1/0/15                Disabled         Disabled
eth1/0/16                Disabled         Disabled
eth1/0/17                Disabled         Disabled
eth1/0/18                Disabled         Disabled
eth1/0/19                Disabled         Disabled
eth1/0/20                Disabled         Disabled
eth1/0/21                Disabled         Disabled
eth1/0/22                Disabled         Disabled
eth1/0/23                Disabled         Disabled
eth1/0/24                Disabled         Disabled
eth1/0/25                Disabled         Disabled
eth1/0/26                Disabled         Disabled
eth1/0/27                Disabled         Disabled
eth1/0/28                Disabled         Disabled

Switch#
```

This example shows how to display the MAC address notification global configuration.

```
Switch#show mac-address-table notification change

MAC Notification Change Feature: Enabled
Interval between Notification Traps: 10 seconds
Maximum Number of Entries Configured in History Table: 500
Current History Table Length: 0
MAC Notification Trap State: Disabled
Trap Type: Without VID

Switch#
```

This example shows how to display the MAC address notification history.

```
Switch# show mac-address-table notification change history

History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 eth1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 eth1/0/1
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 eth1/0/1

Switch#
```

28-11 show multicast filtering-mode

This command is used to display the filtering mode for handling multicast packets that are received on an interface.

show multicast filtering-mode [interface *VLAN-ID***]**

Parameters

interface *VLAN-ID*	(Optional) Specifies the VLAN to display.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the filtering mode for handling multicast packets that are received on an interface.

Example

This example shows how to display the multicast filtering mode configuration for all VLANs.

```
Switch# show multicast filtering-mode

Interface                        Layer 2 Multicast Filtering Mode
-------------------------------  --------------------------------
default                          forward-unregistered

Total Entries: 1

Switch#
```

28-12 snmp-server enable traps mac-notification change

This command is used to enable the sending of SNMP MAC notification traps. Use the **no** form of this command to disable the sending of SNMP MAC notification traps.

snmp-server enable traps mac-notification change

no snmp-server enable traps mac-notification change

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP MAC notification traps.

Example

This example shows how to enable the sending of SNMP MAC notification traps.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps mac-notification change
Switch(config)#
```

28-13 snmp trap mac-notification change

This command is used to enable the MAC address change notification on a specific interface. Use the **no** form of this command to revert to the default setting.

snmp trap mac-notification change {added | removed}

no snmp trap mac-notification change{added | removed}

Parameters

added	Specifies to enable the MAC change notification when a MAC address is added on the interface
removed	Specifies to enable the MAC change notification when a MAC address is removed from the interface.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Even when enabling the notification trap for a specific interface by using the **snmp trap mac-notification change** command, the notification is sent to the notification history table only when the **mac-address-table notification change** command was enabled.

Example

This example shows how to enable the MAC address added notification trap on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)#
```

29. Gratuitous ARP Commands

29-1 ip arp gratuitous

This command is used to enable the learning of gratuitous ARP packets in the ARP cache table. Use the **no** form of this command to disable ARP control.

ip arp gratuitous

no ip arp gratuitous

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The system will learn gratuitous ARP packets in the ARP cache table by default.

Example

This example shows how to disable the learning of gratuitous ARP request packets.

```
Switch# configure terminal
Switch(config)# no ip arp gratuitous
Switch(config)#
```

29-2 ip gratuitous-arps

This command is used to enable the transmission of gratuitous ARP request packets. Use the **no** form of this command to disable the transmission.

ip gratuitous-arps [dad-reply]

no ip gratuitous-arps [dad-reply]

Parameters

dad-reply	(Optional) Specifies control whether the system will reply with another gratuitous ARP request packet with the broadcast DA, when receiving a gratuitous ARP request packet and detecting the duplicate IP address.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

A gratuitous ARP request packet is an ARP request packet where the source and the destination IP address are both set to the IP address of the sending device and the destination MAC address is the broadcast address.

Generally, a device use the gratuitous ARP request packet to discover whether the IP address is duplicated by other hosts or to preload or reconfigure the ARP cache entry of hosts connected to the interface.

Use the **ip gratuitous-arps** command to enable transmission of gratuitous ARP request. The device will send out the packet when an IP interface becomes link-up or when the IP address of an interface is configured or modified.

Use the **ip gratuitous-arps dad-reply** command to enable the transmission of gratuitous ARP requests. The device will send out the packet while a duplicate IP address is detected

Example

This example shows how to sending of gratuitous ARP messages.

```
Switch# configure terminal
Switch(config)# ip gratuitous-arps dad-reply
Switch(config)#
```

29-3 arp gratuitous-send interval

This command is used to set the interval for regularly sending of gratuitous ARP request messages on the interface. Use the **no** form of this command to disable this function on the interface.

arp gratuitous-send interval *SECONDS*

no arp gratuitous-send

Parameters

SECONDS	Specifies the time interval to send the gratuitous ARP request message. The value is from 0 to 3600. 0 represents that this option is disabled.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

If an interface on the Switch is used as the gateway of its downlink devices and counterfeit gateway behavior occurs in the downlink devices, administrators can configure to send gratuitous ARP request messages regularly on this interface to notify that the Switch is the real gateway.

Example

This example shows how to enable the sending of gratuitous ARP messages.

```
Switch# configure terminal
Switch(config)# ip gratuitous-arps
Switch(config)# interface vlan100
Switch(config-if)# arp gratuitous-send interval 1
Switch(config-if)#
```

29-4 snmp-server enable traps gratuitous-arp

This command is used to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected. Use the **no** form of this command to disable the function.

snmp-server enable traps gratuitous-arp

no snmp-server enable traps gratuitous-arp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

Example

This example shows how to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps gratuitous-arp
Switch(config)#
```

30. Interface Commands

30-1 clear counters

This command is used to clear counters for port interfaces.

clear counters {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear counters for all interfaces.
interface *INTERFACE-ID*	Specifies the interfaces to be cleared. Only physical ports are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear counters for port interfaces.

Example

This example shows how to clear the counters on port 1.

```
Switch# clear counters interface eth1/0/1
Switch#
```

30-2 description

This command is used to add a description to an interface. Use the **no** form of this command to delete the description.

description *STRING*

no description

Parameters

STRING	Specifies a description for an interface with a maximum of 64 characters.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Description can be added to any pre-defined interface type. The specified description corresponds to the MIB object “ifAlias” defined in the RFC 2233.

Example

This example shows how to add the description “Physical Port 10” to port 10.

```
Switch# configure terminal
Switch(config)# interface eth1/0/10
Switch(config-if)# description Physical Port 10
Switch(config-if)#
```

This example shows how to add the description “Data VLAN” to Layer 2 Virtual LAN interface.

```
Switch# configure terminal
Switch(config)#interface l2vlan 1
Switch(config-if)#description Data VLAN
Switch(config-if)#
```

30-3 interface

This command is used to enter the Interface Configuration Mode for a single interface. Use the **no** form of this command to remove an interface.

interface *INTERFACE-ID*

no interface *INTERFACE-ID*

Parameters

INTERFACE-ID	Specifies the ID of the interface. The interface ID is formed by interface type and interface number. The interface types are as follows: • **Ethernet** - Ethernet switch port with all different media. • **L2vlan** - IEEE 802.1Q Layer 2 Virtual LAN interface. • **Port-channel** - Aggregated port channel interface. • **Vlan** - VLAN interface.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the Interface Configuration Mode for a specific interface. The format of the interface number is dependent on the interface type. For physical port interfaces, the user cannot enter the interface if the Switch’s port does not exist. The physical port interface cannot be removed by the **no** command.

Use the **interface vlan** command to create Layer 3 interfaces. Use the **vlan** command in the Global Configuration Mode to create a VLAN before creating Layer 3 interfaces. Use the **no interface vlan** command to remove a Layer 3 interface.

The port channel interface is automatically created when the **channel-group** command is configured for the physical port interface. A port channel interface will be automatically removed when no physical port interface has the **channel-group** command configured for it. Use the **no interface port-channel** command to remove a port-channel.

L2vlan interface is only used to add descriptions to existed L2 VLANs. The **interface l2vlan** command does not create any new interface, neither will the no forms of this command removed any existing interface.

Example

This example shows how to enter the Interface Configuration Mode for port 5.

```
Switch# configure terminal
Switch(config)# interface eth1/0/5
Switch(config-if)#
```

This example shows how to enter the interface configuration mode for VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)#
```

This example shows how to enter interface configuration mode for port channel 3.

```
Switch# configure terminal
Switch(config)# interface port-channel 3
Switch(config-if)#
```

30-4 interface range

This command is used to enter the Interface Range Configuration Mode for multiple interfaces.

interface range *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the ID of the interface. The interface ID is formed by interface type and interface number. The interface types are as follows: • **Ethernet** - Ethernet switch port with all different media. • **L2vlan** - IEEE 802.1Q Layer 2 Virtual LAN interface.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the Interface Range Configuration Mode for the specified range of interfaces. All Commands configured in the Interface Range Configuration Mode apply to all interfaces specified in the range.

Example

This example shows how to enter the Interface Range Configuration Mode for ports 1 to 5 and port 8.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

30-5 show counters

This command is used to display interface information.

show counters [interface *INTERFACE-ID* **[- | ,]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed. If not specified, the counters on all interfaces will be displayed. Only physical ports are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the statistic counters for the specified interface(s).

Example

This example shows how to display the counters on port 1.

```
Switch#show counters interface eth1/0/1

eth1/0/1 counters
rxHCTotalPkts                    : 1549
txHCTotalPkts                    : 154322
rxHCUnicastPkts                  : 1319
txHCUnicastPkts                  : 473
rxHCMulticastPkts                : 78
txHCMulticastPkts                : 78572
rxHCBroadcastPkts                : 152
txHCBroadcastPkts                : 75277
rxHCOctets                       : 135984
txHCOctets                       : 16607644
rxHCPkt64Octets                  : 244
rxHCPkt65to127Octets             : 1176
rxHCPkt128to255Octets            : 110
rxHCPkt256to511Octets            : 15
rxHCPkt512to1023Octets           : 3
rxHCPkt1024to1518Octets          : 1
rxHCPkt1519to1522Octets          : 0
rxHCPkt1519to2047Octets          : 0
rxHCPkt2048to4095Octets          : 0
rxHCPkt4096to9216Octets          : 0
rxHCPkt9217to16383Octets         : 0
txHCPkt64Octets                  : 132105
txHCPkt65to127Octets             : 1531
txHCPkt128to255Octets            : 2120
txHCPkt256to511Octets            : 13794
txHCPkt512to1023Octets           : 4712
txHCPkt1024to1518Octets          : 60
txHCPkt1519to1522Octets          : 0
txHCPkt1519to2047Octets          : 0
txHCPkt2048to4095Octets          : 0
txHCPkt4096to9216Octets          : 0
txHCPkt9217to16383Octets         : 0

rxCRCAlignErrors                 : 0
rxUndersizedPkts                 : 0
rxOversizedPkts                  : 0
rxFragmentPkts                   : 0
rxJabbers                        : 0
rxSymbolErrors                   : 0
rxBufferFullDropPkts             : 0
rxACLDropPkts                    : 0
rxMulticastDropPkts              : 0
rxVLANIngressCheckDropPkts       : 0
rxIpv6DropPkts                   : 0
rxSTPDropPkts                    : 0
rxStormAndTableDropPkts          : 0
rxMTUDropPkts                    : 0

txCollisions                     : 0
ifInErrors                       : 0
ifOutErrors                      : 0
```

```
ifInDiscards                    : 0
ifOutDiscards                   : 0
ifInUnknownProtos               : 0
txDelayExceededDiscards         : 0
txCRC                           : 0
txSTPDropPkts                   : 0
txHOLDropPkts                   : 0
txCoS0DropPkts                  : 0
txCoS1DropPkts                  : 0
txCoS2DropPkts                  : 0
txCoS3DropPkts                  : 0
txCoS4DropPkts                  : 0
txCoS5DropPkts                  : 0
txCoS6DropPkts                  : 0
txCoS7DropPkts                  : 0

dot3StatsAlignmentErrors        : 0
dot3StatsFCSErrors              : 0
dot3StatsSingleColFrames        : 0
dot3StatsMultiColFrames         : 0
dot3StatsSQETestErrors          : 0
dot3StatsDeferredTransmissions  : 0
dot3StatsLateCollisions         : 0
dot3StatsExcessiveCollisions    : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsCarrierSenseErrors     : 0
dot3StatsFrameTooLongs          : 0
dot3StatsInternalMacReceiveErrors  : 0

linkChange                      : 5


Switch#
```

Display Parameters

rxHCTotalPkts	Receive Packet Counter. Incremented for each packet received (includes bad packets, all Unicast, Broadcast, Multicast Packets, and MAC control packets).
txHCTotalPkts	Transmit Packet Counter. Incremented for each packet transmitted (including bad packets, all Unicast, Broadcast, Multicast packets and MAC control packets).
rxHCUnicastPkts	Receive Unicast Packet Counter. Incremented for each good unicast packet received.
txHCUnicastPkts	Transmit Unicast Packet Counter. Incremented for each good unicast packet transmitted.
rxHCMulticastPkts	Receive Multicast Packet Counter. Incremented for each good Multicast packet received. (Excluding MAC control packets).
txHCMulticastPkts	Transmit Multicast Packet Counter. Incremented for each good Multicast packet transmitted. (Excluding MAC control frames).
rxHCBroadcastPkts	Receive Broadcast Packet Counter. Incremented for each good Broadcast packet received.
txHCBroadcastPkts	Transmit Broadcast Packet Counter. Incremented for each good Broadcast packet transmitted.

rxHCOctets	Receive Byte Counter. Incremented by the byte count of packets received, including bad packets. (Excluding framing bits but including FCS bytes). Note: For truncated packet, the counter only counts up to max-rcv-frame-size size.
txHCOctets	Transmit Byte Counter. Incremented for the bytes of packets transmitted. (Excluding framing bits but including FCS bytes).
rxHCPkt64Octets	Receive 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt65to127Octets	Receive 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt128to255Octets	Receive 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt256to511Octets	Receive 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len /Type error) frame received which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt512to1023Octets	Receive 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt1024to1518Octets	Receive 1024 to 1518 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 1024 to 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt1519to1522Octets	Receive 1519 to 1522 Byte Good VLAN Frame Counter. Incremented for each good VLAN (excludes FCS, Symbol, Truncated error) frame received which is 1519 to 1522 bytes in length inclusive (excluding framing bits but including FCS bytes). Counts both single and double tag frames.
rxHCPkt1519to2047Octets	Receive 1519 to 2047 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 1519 to 2047 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt2048to4095Octets	Receive 2048 to 4095 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 2048 to 4095 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt4096to9216Octets	Receive 4096 to 9216 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 4096 to 9216 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt9217to16383Octets	Receive 9217 to 16383 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 9217 to 16383 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt64Octets	Transmit 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes).

txHCPkt65to127Octets	Transmit 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt128to255Octets	Transmit 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt256to511Octets	Transmit t 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt512to1023Octets	Transmit 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1024to1518Octets	Transmit 1024 to 1518 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 1024 to 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1519to2047Octets	Transmit 1519 to 2047 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 1519 to 2047 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt2048to4095Octets	Transmit 2048 to 4095 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 2048 to 4095 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt4096to9216Octets	Transmit 4096 to 9216 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 4096 to 9216 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt9217to16383Octets	Transmit 9217 to 16383 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 9217 to 16383 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxCRCAlignErrors	Receive Alignment Error Frame Counter. Incremented for each packet received which is 64 to max-rcv-frame-size (or max-rcv-frame-size+4 for tagged frames) octets in length (excluding framing bits, but including FCS octets), but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxUndersizedPkts	Receive Undersize Frame Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contains a valid FCS).
rxOversizedPkts	Receive Oversized Frame Counter. Incremented for each packet received which is longer than 1518 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contain a valid FCS).
rxFragmentPkts	Receive Fragment Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxJabbers	Receive Jabber Frame Counter. Incremented for each packet received which is longer than 1518 bytes in length (excluding framing bits, but

	including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxSymbolErrors	Receive Code Error Frame Counter. Incremented for the count of times where there was an invalid data symbol when a valid carrier was present.
rxBufferFullDropPkts	Receive Discard Packet Counter. Incremented for each packet discarded for input buffer (GBP) full or back pressure discard.
rxACLDropPkts	Receive ACL Drop Packet Counter. Incremented for each packet that was dropped by ACL rules.
rxMulticastDropPkts	Receive Multicast Drop Packet Counter. Incremented for each multicast (including Layer 2 and Layer 3) packets that was dropped.
rxVLANIngressCheckDropPkts	Receive VLAN Drop Packet Counter. Incremented for each packet that was dropped by VLAN ingress checking.
rxIpv6DropPkts	Receive IPv6 L3 Drop Packet Counter. Incremented for each packet addressed to L3 interface, which are discarded due to the following reasons: RX Buffer hits the Receive Discard Limit or GBP full.
rxSTPDropPkts	Receive STP Drop Packet Counter. Incremented for packets dropped due to Spanning Tree State of ingress port was not in forwarding state.
rxStormAndTableDropPkts	Receive Policy Discard Packet Counter. Incremented for packets dropped due to receive policy: storm control action, FDB action, and so on.
rxMTUDropPkts	Receive MTU Check Error Frame Counter. Incremented for each frame received which exceeds the max-rcv-frame-size in length and contain a valid or invalid FCS. Note: Single VLAN tagged, truncation happens at max-rcv-frame-size +4; double VLAN tagged, truncation happens at max-rcv-frame-size +8.
txCollisions	Transmit Total Collision Counter. Incremented by the total number of collisions experienced during the transmission.
ifInErrors	Received Error Packet Counter. Incremented for received packets which contained errors preventing them from being deliverable to a higher-layer protocol. The counter is the sum of dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveTransmitErrors, dot3StatsSymbolErrors, undersize, fragment, oversize, and jabber error.
ifOutErrors	Transmit Error Packet Counter. Incremented for outbound packets which could not be transmitted because of errors. The counter is the sum of dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors, and dot3StatsCarrierSenseErrors.
ifInDiscards	Receive Discards Packet Counter. Incremented for packets received which are dropped due to any condition. Such as MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard, and etc.
ifOutDiscards	Transmit Discards Packet Counter. Incremented for packets transmitted which are dropped due to any condition. Such as excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop, and etc.
ifInUnknownProtos	Receive Discards Unknown and Unsupported protocol Counter. Incremented for packets received, which were discarded because of an unknown or unsupported protocol.

txDelayExceededDiscards	Transmit Multiple Deferral Packet Counter. Incremented for packets transmitted which are discarded due to excessive transit delay.
txCRC	Transmit FCS Error Packet Counter. Incremented for each frame transmitted which does not pass the FCS check.
txSTPDropPkts	Transmit STP Drop Packet Counter. Incremented for packets dropped due to Spanning Tree State of egress port was not in forwarding state.
txHOLDropPkt	Transmit HOL Drop Packet Counter. Incremented for each packet drop due to Head Of Line blocking.
txCoS0DropPkts	Transmit COS 0 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 0.
txCoS1DropPkts	Transmit COS 1 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 1.
txCoS2DropPkts	Transmit COS 2 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 2.
txCoS3DropPkts	Transmit COS 3 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 3.
txCoS4DropPkts	Transmit COS 4 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 4.
txCoS5DropPkts	Transmit COS 5 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 5.
txCoS6DropPkts	Transmit COS 6 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 6.
txCoS7DropPkts	Transmit COS 7 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 7.
dot3StatsAlignmentErrors	Receive Alignment Error Frame Counter. Incremented for each frame received which are not an integral number of octets in length and does not pass the FCS check. Note: Whether dot3StatsAlignmentErrors could be counted is ASIC dependent.
dot3StatsFCSErrors	Receive FCS Error Frame Counter. Incremented for each packet received which is an integral number of octets in length but do not pass the FCS check. Note: Whether dot3StatsFCSErrors could be counted is ASIC dependent.
dot3StatsSingleColFrames	Transmit Single Collision Frame Counter. 10/100 mode only - incremented for each frame transmitted which experienced exactly one collision during transmission.
dot3StatsMultiColFrames	Transmit Multiple Collision Frame Counter. 10/100 mode only - incremented for each frame successfully transmitted for which transmission is inhibited by more than one collision.
dot3StatsSQETestErrors	SQET Test Error Counter. Incremented for times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document. Note: This counter does not increment at speeds greater than 10 Mb/s, or in full-duplex mode.
dot3StatsDeferredTransmissions	Transmit Single Deferral Frame Counter. 10/100 mode only - incremented for each frame which was deferred on its first transmission attempt and did not experience any subsequence collisions during transmission.
dot3StatsLateCollisions	Transmit Late Collision Frame Counter.

	10/100 mode only - incremented for each frame transmitted which experienced a late collision during a transmission attempt.
dot3StatsExcessiveCollisions	Transmit Excessive Collision Frame Counter. 10/100 mode only - incremented for each frame transmitted for which transmission fails due to excessive collisions.
dot3StatsInternalMacTransmitErrors	Transmit Internal MAC Error Frame counter. Incremented for frames for which transmission fails due to an internal MAC sublayer transmitting error. A frame is only counted if it is not counted by any of the dot3StatsLateCollisions, the dot3StatsExcessiveCollisions, and the dot3StatsCarrierSenseErrors.
dot3StatsCarrierSenseErrors	False Carrier Counter. Incremented for times that the carrier sense condition was lost or never asserted when attempting to transmit a frame. Note: Whether dot3StatsCarrierSenseErrors could be counted is ASIC dependent.
dot3StatsFrameTooLongs	Receive Frame Too Long Counter. Incremented for each frame received which exceeds the max-rcv-frame-size.
dot3StatsInternalMacReceiveErrors	Receive Internal MAC Error counter. Incremented for frames for which reception fails due to an internal MAC sublayer receiving error. A frame is only counted if it is not counted by the corresponding instance of any of the dot3StatsFrameTooLongs, the dot3StatsAlignmentErrors, or the dot3StatsFCSErrors.

30-6 show interfaces

This command is used to display the interface information.

show interfaces [*INTERFACE-ID* **[- | ,]]**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all existing physical ports will be displayed.

Example

This example shows how to display the VLAN 1 interface information.

```
Switch#show interfaces vlan1

Vlan1 is enabled, Link status is down
  Interface type: VLAN
  MAC address: F0-7D-68-12-10-01



Switch#
```

This example shows how to display the interface information for port 1.

```
Switch#show interfaces eth1/0/1

Eth1/0/1 is enabled, link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 00-01-02-03-04-01
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1536 bytes
  Rx rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 116316, TX bytes: 132495
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 1213, TX packets: 365
  RX multicast: 774, RX broadcast: 439
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 1212
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision:0

Switch#
```

30-7 show interfaces counters

This command is used to display counters on specified interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] counters [errors]**

Parameters

INTERFACE-ID	(Optional) pecifies the interfaces to be displayed. If no interface is specified, the counters on all interfaces will be displayed. Only physical ports are allowed to be specified.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
errors	(Optional) Specifies to display the error counters.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display switch port statistics counters.

Example

This example shows how to display switch port counters on ports 1 to 8.

```
Switch# show interfaces eth1/0/1-8 counters

Port          InOctets /            InMcastPkts /
              InUcastPkts           InBcastPkts
------------- --------------------- ---------------------
eth1/0/1      1834520               629
              9234                  338
eth1/0/2      0                     0
              0                     0
eth1/0/3      0                     0
              0                     0
eth1/0/4      0                     0
              0                     0
eth1/0/5      0                     0
              0                     0
eth1/0/6      0                     0
              0                     0
eth1/0/7      0                     0
              0                     0
eth1/0/8      0                     0
              0                     0

Port          OutOctets /           OutMcastPkts /
              OutUcastPkts          OutBcastPkts
------------- --------------------- ---------------------
eth1/0/1      5387265               0
              9381                  0
eth1/0/2      0                     0
              0                     0
eth1/0/3      0                     0
              0                     0
eth1/0/4      0                     0
              0                     0
eth1/0/5      0                     0
              0                     0
eth1/0/6      0                     0
              0                     0
eth1/0/7      0                     0
              0                     0
eth1/0/8      0                     0
              0                     0

Total Entries:8

Switch#
```

This example shows how to display switch ports error counters.

```
Switch#show interfaces eth1/0/1 counters errors

Port            Align-Err /           Fcs-Err /
                Rcv-Err /             Undersize /
                Xmit-Err              OutDiscard
--------------- --------------------- ---------------------
eth1/0/1        0                     0
                0                     0
                0                     0

Port            Single-Col /          Excess-Col /
                Multi-Col /           Carri-Sen /
                Late-Col              Runts
--------------- --------------------- ---------------------
eth1/0/1        0                     0
                0                     0
                0                     0

Port            Giants /              DeferredTx /
                Symbol-Err /          IntMacTx /
                SQETest-Err           IntMacRx
--------------- --------------------- ---------------------
eth1/0/1        0                     0
                0                     0
                0                     0

Total Entries:1


Switch#
```

Display Parameters

Align-Err	Refer to the item “dot3StatsAlignmentErrors” in the **show counters** command.
Rcv-Err	Refer to the item “ifInErrors” in Display Parameters in the **show counters** command.
Xmit-Err	Refer to the item “ifOutErrors” in Display Parameters in the **show counters** command.
Fcs-Err	Refer to the item “dot3StatsFCSErrors” in the **show counters** command.
UnderSize	Refer to the item “rxUndersizedPkts” in Display Parameters in the **show counters** command.
OutDiscard	Refer to the item “ifOutDiscards” in Display Parameters in the **show counters** command.
Single-Col	Refer to the item “dot3StatsSingleColFrames” in Display Parameters in the **show counters** command.
Multi-Col	Refer to the item “dot3StatsMultiColFrames” in Display Parameters in the **show counters** command.
Late-Col	Refer to the item “dot3StatsLateCollisions” in Display Parameters in the **show counters** command.
Excess-Col	Refer to the item “dot3StatsExcessiveCollisions” in Display Parameters in the **show counters** command.
Carri-Sen	Refer to the item “dot3StatsCarrierSenseErrors” in the **show counters** command.

Runts	Incremented for each packet whose size is less than 64 bytes in length.
Giants	Incremented for each packet whose size is greater than 1518 bytes in length.
Symbol-Err	Refer to the item “rxSymbolErrors” in Display Parameters in the **show counters** command.
SQETest-Err	Refer to the item “dot3StatsSQETestErrors” in the **show counters** command.
DeferredTx	Refer to the item “txDelayExceededDiscards” in Display Parameters in the **show counters** command.
IntMacTx	Refer to the item “dot3StatsInternalMacTransmitErrors” in Display Parameters in the **show counters** command.
IntMacRx	Refer to the item “dot3StatsInternalMacReceiveErrors” in the **show counters** command.

30-8 show interfaces status

This command is used to display the port connection status of the Switch.

show interfaces [*INTERFACE-ID* **[, | -]] status**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the port connection status of the Switch. If no parameter is specified, the connection status of all switch ports will be displayed.

Example

This example shows how to display the port connection status of the Switch.

```
Switch#show interfaces eth1/0/1-8 status

Port          Status        VLAN         Duplex  Speed          Type
------------- ------------- ------------ ------- -------------- -------------
eth1/0/1      connected     1            a-full  a-100          10GBASE-T
eth1/0/2      not-connected 1            auto    auto           10GBASE-T
eth1/0/3      connected     1            a-full  a-100          10GBASE-T
eth1/0/4      not-connected 1            auto    auto           10GBASE-T
eth1/0/5      not-connected 1            auto    auto           10GBASE-T
eth1/0/6      not-connected 1            auto    auto           10GBASE-T
eth1/0/7      not-connected 1            auto    auto           10GBASE-T
eth1/0/8      not-connected 1            auto    auto           10GBASE-T

Total Entries: 8


Switch#
```

30-9 show interfaces utilization

This command is used to display the port utilization of the Switch.

show interfaces [*INTERFACE-ID* **[, | -]] utilization**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed. If no interface is specified, the utilization of all physical port interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
utilization	Specifies to display the utilization information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the port utilization of the Switch.

Example

This example shows how to display the port utilization of the Switch.

```
Switch#show interfaces eth1/0/1-8 utilization

Port           TX packets/sec    RX packets/sec    Utilization
-------------  ----------------- ----------------- -----------
eth1/0/1       2                 0                 1
eth1/0/2       0                 0                 0
eth1/0/3       0                 2                 1
eth1/0/4       0                 0                 0
eth1/0/5       0                 0                 0
eth1/0/6       0                 0                 0
eth1/0/7       0                 0                 0
eth1/0/8       0                 0                 0

Total Entries:8


Switch#
```

30-10 show interfaces auto-negotiation

This command is used to display detailed auto-negotiation information of physical port interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] auto-negotiation**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed. If no interface is specified, the auto-negotiation information on all physical port interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
auto-negotiation	Specifies to display detailed auto-negotiation information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display auto-negotiation information.

Example

This example shows how to display auto-negotiation information.

```
Switch#show interfaces eth1/0/1-2 auto-negotiation

eth1/0/1
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Complete
 Capability Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Advertised Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError

eth1/0/2
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Configuring
 Capability Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Advertised Bits: 100M_Full, 1000M_Full, 10G_Full
 Capability Received Bits: -
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


Switch#
```

30-11 show interfaces description

This command is used to display the description and link status of interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] description**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed. If no interface is specified, the information of all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
description	Specifies to display the description and link status of interfaces.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the description and link status of interfaces.

Example

This example shows how to display the description and link status of interfaces.

```
Switch# show interfaces description

 Interface              Status    Administrative  Description
 ---------------------  --------  --------------  ------------------------------
 eth1/0/1               up        enabled
 eth1/0/2               down      enabled
 eth1/0/3               up        enabled
 eth1/0/4               down      enabled
 eth1/0/5               down      enabled
 eth1/0/6               down      enabled
 eth1/0/7               down      enabled
 eth1/0/8               down      enabled
 eth1/0/9               down      enabled
 eth1/0/10              down      enabled         Physical Port 10
 eth1/0/11              down      enabled
 eth1/0/12              down      enabled
 eth1/0/13              down      enabled
 eth1/0/14              down      enabled
 eth1/0/15              down      enabled
 eth1/0/16              down      enabled
 eth1/0/17              down      enabled
 eth1/0/18              down      enabled
 eth1/0/19              down      enabled
 eth1/0/20              down      enabled
 eth1/0/21              down      enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

30-12 shutdown

This command is used to disable an interface. Use the **no** form of this command to enable an interface.

shutdown

no shutdown

Parameters

None.

Default

By default, this option is **no shutdown**.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is available for physical port and VLAN interface configuration. This command is also configurable for port channel member ports.

The command will cause the port to enter the disabled state. Under the disabled state, the port will not be able to receive or transmit any packets. Using the **no shutdown** command will put the port back into the enabled state. When a port is shut down, the link status will also be turned off.

Example

This example shows how to disable the port state on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# shutdown
```

30-13 max-rcv-frame-size

This command is used to configure the maximum Ethernet frame size allowed. Use the **no** form of this command to revert to the default setting.

max-rcv-frame-size *BYTES*

no max-rcv-frame-size

Parameters

BYTES	Specifies the maximum Ethernet frame size allowed. The range is from 64 to 12288 bytes.

Default

By default, this value is 1536 bytes.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Oversize frames will be dropped and checks are carried out on ingress ports. Use this command to transfer large frames or jumbo frames through the switch system to optimize server-to-server performance.

Example

This example shows how to configure the maximum received Ethernet frame size to be 6000 bytes on port 3.

```
Switch# configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

31. Internet Group Management Protocol (IGMP) Snooping Commands

31-1 clear ip igmp snooping statistics

This command is used to clear the IGMP snooping related statistics.

clear ip igmp snooping statistics {all | vlan *VLAN-ID* **| interface** *INTERFACE-ID***}**

Parameters

all	Specifies to clear IP IGMP snooping statistics for all VLANs and all ports.
vlan *VLAN-ID*	Specifies a VLAN to clear the IP IGMP snooping statistics.
interface *INTERFACE-ID*	Specifies a port to clear the IP IGMP snooping statistics.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the IGMP snooping related statistics.

Example

This example shows how to clear all IGMP Snooping statistics.

```
Switch#clear ip igmp snooping statistics all
Switch#
```

31-2 ip igmp snooping

This command is used to enable the IGMP snooping function on the Switch. Use the **no** form of this command to disable the IGMP snooping function.

ip igmp snooping

no ip igmp snooping

Parameters

None.

Default

IGMP snooping is disabled on all VLANs.

The IGMP snooping global state is disabled by default.

Command Mode

VLAN Configuration Mode.

Global Configuration Mode.

Usage Guideline

For a VLAN to operate with IGMP snooping, both the global state and per VLAN state must be enabled. On a VLAN, the setting of IGMP snooping and MLD snooping are independent. IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

Example

This example shows how to disable the IGMP snooping globally.

```
Switch# configure terminal
Switch(config)# no ip igmp snooping
Switch(config)#
```

This example shows how to enable the IGMP snooping globally.

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)#
```

This example shows how to disable IGMP snooping on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping
Switch(config-vlan)#
```

31-3 ip igmp snooping fast-leave

This command is used to configure IGMP snooping fast-leave. Use the **no** form to disable the fast-leave option.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to allow IGMP membership to be immediately removed from a port when receiving the leave message without using the group specific or group-source specific query mechanism.

Example

This example shows how to enable IGMP snooping fast-leave on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping fast-leave
Switch(config-vlan)#
```

31-4 ip igmp snooping last-member-query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

ip igmp snooping last-member-query-interval *SECONDS*

no ip igmp snooping last-member-query-interval

Parameters

SECONDS	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

VLAN Configuration Mode.

Usage Guideline

On receiving an IGMP leave message, the IGMP snooping querier will assume that there are no local members in the VLAN if there are no reports received after the response time. Users can lower this interval to reduce the amount of time it takes a switch to detect the loss of the last member of a group.

Example

This example shows how to configure the last member query interval time to be 3 seconds.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping last-member-query-interval 3
Switch(config-vlan)#
```

31-5 ip igmp snooping minimum-version

This command is used to configure the minimum version of IGMP hosts that is allowed in the VLAN. Use the **no** form of this command to remove the restriction from the VLAN.

ip igmp snooping minimum-version *NUMBER*

no ip igmp snooping minimum-version

Parameters

NUMBER	Specifies the minimum version of IGMP hosts. • **2** - Specifies to filter out IGMPv1 messages. • **3** - Specifies to filter out IGMPv1 and IGMPv2 messages.

Default

By default, there is no limit on the minimum version.

Command Mode

VLAN Configuration Mode.

Usage Guideline

This setting only applies to the filtering of IGMP membership reports.

Example

This example shows how to restrict all IGMPv1 hosts to join VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping minimum-version 2
Switch(config-vlan)#
```

This example shows how to restrict all IGMPv1 and IGMPv2 hosts disallowed to join VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping minimum-version 3
Switch(config-vlan)#
```

This example shows how to remove the restriction configured on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping minimum-version
Switch(config-vlan)#
```

31-6 ip igmp snooping mrouter

This command is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden multicast router ports.

ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

no ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

Parameters

interface	Specifies a static multicast router port.
forbidden interface	Specifies a port that cannot be multicast router port.

INTERFACE-ID	Specifies an interface or an interface list. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No IGMP snooping multicast router port is configured.

Command Mode

VLAN Configuration Mode.

Usage Guideline

To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be member port of the configured VLAN. A multicast router port can be either dynamic learned or statically configured. With the dynamic learning, the IGMP snooping entity will learn IGMP, PIM, or DVMRP packet to identify a multicast router port.

Example

This example shows how to dd an IGMP snooping static multicast router port for VLAN 1.

```
Switch#configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping mrouter interface eth1/0/4
Switch(config-vlan)#
```

31-7 ip igmp snooping querier

This command is used to enable the capability of the entity as an IGMP querier. Use the **no** form of this command to disable the querier function.

ip igmp snooping querier

no ip igmp snooping querier

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

If the system can play the querier role, the entity will listen for IGMP query packets sent by other devices. If IGMP query message is received, the device with lower value of IP address becomes the querier.

Example

This example shows how to enable the IGMP snooping querier on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping querier
Switch(config-vlan)#
```

31-8 ip igmp snooping query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP general query messages periodically. Use the **no** form of this command to revert to the default setting.

ip igmp snooping query-interval *SECONDS*

no ip igmp snooping query-interval

Parameters

SECONDS	Specifies to configure the interval at which the designated router sends IGMP general-query messages. The range is 1 to 31744.

Default

By default, this value is 125 seconds.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The query interval is the interval between General Queries sent by the Querier. By varying the query interval, an administrator may tune the number of IGMP messages on the network; larger values cause IGMP Queries to be sent less often.

Example

This example shows how to configure the IGMP snooping query interval to 300 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-interval 300
Switch(config-vlan)#
```

31-9 ip igmp snooping query-max-response-time

This command is used to configure the maximum response time advertised in IGMP snooping queries. Use the **no** form of this command to revert to the default setting.

ip igmp snooping query-max-response-time *SECONDS*

no ip igmp snooping query-max-response-time

Parameters

SECONDS	Specifies to set the maximum response time, in seconds, advertised in IGMP snooping queries. The range is 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to configure the period of which the group member can respond to an IGMP query message before the IGMP Snooping deletes the membership.

This group membership life-time is calculated as follows: query-interval x robustness + max response time.

Example

This example shows how to configure the maximum response time to 20 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-max-response-time 20
Switch(config-vlan)#
```

31-10 ip igmp snooping query-version

This command is used to configure the general query packet version sent by the IGMP snooping querier. Use the **no** form of this command to revert to the default setting.

ip igmp snooping query-version *NUMBER*

no ip igmp snooping query-version

Parameters

NUMBER	Specifies the version of the IGMP general query sent by the IGMP snooping querier. The value is from 1 to 3.

Default

By default, this value is 3.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The query version number setting will affect the querier electing. When configured to version 1, IGMP snooping will always act as the querier, and will not initiate new querier electing no matter what IGMP query packet is received. When configured to version 2 or version 3, IGMP snooping will initiate a new querier electing if any IGMPv2 or IGMPv3 query packet is received. When receiving an IGMPv1 query packet, IGMP snooping will not initiate a new querier electing.

Example

This example shows how to configure the query version to be 2 on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-version 2
Switch(config-vlan)#
```

31-11 ip igmp snooping report-suppression

This command is used to enable the report suppression. Use the **no** form of this command to disable the report suppression.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expired. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.

Example

This example shows how to enable report suppression on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping report-suppression
Switch(config-vlan)#
```

31-12 ip igmp snooping robustness-variable

This command is used to set the robustness variable used in IGMP snooping. Use the **no** form of this command to revert to the default setting.

ip igmp snooping robustness-variable *VALUE*

no ip igmp snooping robustness-variable

Parameters

VALUE	Specifies the robustness variable. The range is from 1 to 7.

Default

By default, this value is 2.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The robustness variable provides fine-tuning to allow for expected packet loss in the VLAN. The value of the robustness variable is used in calculating the following IGMP message intervals:

- **Group member interval** - The amount of time that must pass before a multicast router decides there are no more members of a group on a network.

  This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).

- **Other querier present interval** - The amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier.

  This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).

- **Last member query count** - The number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable.

Users can increase this value if a subnet is expected to be loose.

Example

This example shows how to configure the robustness variable to be 3 on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

31-13 ip igmp snooping static-group

This command is used to configure an IGMP snooping static group. Use the **no** form of this command is used to delete a static group.

ip igmp snooping static-group *GROUP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ip igmp snooping static-group *GROUP-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

GROUP-ADDRESS	Specifies an IP multicast group address.
interface *INTERFACE-ID*	Specifies the interfaces to be displayed. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, no static-group is configured.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to create an IGMP snooping static group in case that the attached host does not support the IGMP protocol.

Example

This example shows how to statically add a group for IGMP snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface eth1/0/5
Switch(config-vlan)#
```

31-14 ip igmp snooping suppression-time

This command is used to configure the time for suppressing duplicate IGMP reports or leaves. Use the **no** form of this command to revert to the default setting.

ip igmp snooping suppression-time *SECONDS*

no ip igmp snooping suppression-time

Parameters

SECONDS	Specifies to configure the time for suppressing duplicates IGMP reports. The range is from 1 to 300.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The report suppression function will suppress the duplicate IGMP report or leave packets received in the suppression time. A small suppression time will cause the duplicate IGMP packets be sent more frequently.

Example

This example shows how to configure the suppression time to be 125 on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping suppression-time 125
Switch(config-vlan)#
```

31-15 show ip igmp snooping

This command is used to display IGMP snooping information on the Switch.

show ip igmp snooping [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display IGMP snooping information for all VLANs where IGMP snooping is enabled.

Example

This example shows how to display IGMP snooping global state.

```
Switch# show ip igmp snooping

IGMP snooping global state: Enabled

Switch#
```

This example shows how to display IGMP snooping information on VLAN 1.

```
Switch#show ip igmp snooping vlan 1

VLAN #1 configuration
    IGMP snooping state             : Disabled
    Minimum version                 : v1
    Fast leave                      : Disabled (port-based)
    Report suppression              : Disabled
    Suppression time                : 10 seconds
    Querier state                   : Disabled
    Query version                   : v3
    Query interval                  : 125 seconds
    Max response time               : 10 seconds
    Robustness value                : 2
    Last member query interval      : 1 seconds

Total Entries: 1

Switch#
```

31-16 show ip igmp snooping groups

This command is used to display IGMP snooping dynamic group information learned on the Switch.

show ip igmp snooping groups [vlan *VLAN-ID* **[, | -] | [***IP-ADDRESS***] [detail]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN interface to be displayed. If no VLAN is specified, IGMP snooping group information of all IGMP snooping-enabled VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
IP-ADDRESS	(Optional) Specifies the group IP address to be displayed. If no IP address is specified, all IGMP group information will be displayed.
detail	(Optional) Specifies to display the IGMP group detail information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display IGMP snooping dynamic group information.

Example

This example shows how to display IGMP snooping dynamic group information.

```
Switch#show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: eth1/0/3,eth1/0/5

Switch#
```

This example shows how to display IGMP snooping group detail information.

```
Switch#show ip igmp snooping groups detail

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: eth1/0/3,eth1/0/5
  eth1/0/3
    version: v2, filter mode: Exclude, uptime: 0DT00H00M05S, expires: 0DT00H04M16S
  eth1/0/5
    version: v3, filter mode: Include, uptime: 0DT00H00M07S, expires: 0DT00H00M00S
      source 192.168.1.1, uptime: 0DT00H00M07S, expires: 0DT00H04M13S

Switch#
```

31-17 show ip igmp snooping mrouter

This command is used to display IGMP snooping router port information learned and configured on the Switch.

show ip igmp snooping mrouter [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed. If no VLAN is specified, IGMP snooping information on all VLANs will be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

If no parameter is specified, IGMP snooping information on all VLANs will be displayed.

Example

This example shows how to display IGMP snooping router port information on VLAN 1.

```
Switch#show ip igmp snooping mrouter vlan 1

VLAN   Ports
-----  ----------------------------
1      eth1/0/7 (static)

Total Entries: 1

Switch#
```

31-18 show ip igmp snooping static-group

This command is used to display statically configured IGMP snooping groups on the Switch.

show ip igmp snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IP address to be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display statically configured IGMP snooping groups on the Switch. If no parameter is specified, all information will be displayed.

Example

This example shows how to display IGMP snooping static group information.

```
Switch#show ip igmp snooping static-group

VLAN ID  Group address    Interface
-------  ---------------  ------------------------
1        230.1.1.1        eth1/0/2-1/0/5

Total Entries: 1

Switch#
```

31-19 show ip igmp snooping statistics

This command is used to display IGMP snooping statistics information on the Switch.

show ip igmp snooping statistics {interface [*INTERFACE-ID* **[, | -]] | vlan [***VLAN-ID* **[, | -]]}**

Parameters

interface	Specifies to display statistics counters by interface. Only physical port and port-channel interfaces are allowed.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan	Specifies to display statistics counters by VLAN.

VLAN-ID	(Optional) Specifies the VLAN ID to be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command displays the IGMP snooping related statistics information.

Example

This example shows how to display IGMP snooping statistics information.

```
Switch#show ip igmp snooping statistics vlan 1


VLAN 1 Statistics:
  IGMPv1 Rx: Report 0, Query 0
  IGMPv2 Rx: Report 0, Query 0, Leave 0
  IGMPv3 Rx: Report 3, Query 0
  IGMPv1 Tx: Report 0, Query 0
  IGMPv2 Tx: Report 0, Query 0, Leave 0
  IGMPv3 Tx: Report 1, Query 2

Total Entries: 1

Switch#
```

32. IP-MAC-Port Binding (IMPB) Commands

32-1 clear ip ip-mac-port-binding violation

This command is used to clear IMPB blocked entries.

clear ip ip-mac-port-binding violation {all | interface *INTERFACE-ID* **|** *MAC-ADDRESS***}**

Parameters

all	Specifies to clear all of the violation entries.
interface *INTERFACE-ID*	Specifies to clear the violation entries created by the specified interface.
MAC-ADDRESS	Specifies to clear the violation entries of the specified MAC address.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to delete the IMPB violation entry from the filtering database.

Example

This example shows how to clear the entry blocked on port 4.

```
Switch# clear ip ip-mac-port-binding violation interface eth1/0/4
Switch#
```

32-2 ip ip-mac-port-binding

This command is used to enable the IMPB access control for port interfaces. Use the **no** form of this command to disable the IMPB access control function.

ip ip-mac-port-binding [*MODE***]**

no ip ip-mac-port-binding

Parameters

MODE	(Optional) Specifies the IMPB access control mode. • **strict-mode** - Specifies to perform strict mode access control. • **loose-mode** - Specifies to perform loose mode access control. If not specified, the **strict-mode** is used.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

When a port is enabled for IMPB **strict-mode** access control, a host can only access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host passes the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port number must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

When a port is enabled for IMPB **loose-mode** access control, a host will be denied to access the port after the host sends ARP or IP packets and the ARP packet or IP packet sent by the host does not pass the binding check. To pass the binding check, the source IP address, source MAC address, VLAN ID, and arrival port must match any of the entries defined by either the IP source guard static binding entry or the DHCP snooping learned dynamic binding entry.

Example

This example shows how to enable the strict-mode IMPB access control on port 10.

```
Switch# configure terminal
Switch(config)# interface eth1/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

32-3 show ip ip-mac-port-binding

This command is used to display the IMPB configuration settings or the entries blocked by IMPB access control.

show ip ip-mac-port-binding [interface *INTERFACE-ID* **[, | -]] [violation]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
violation	(Optional) Specifies to display the blocked entry.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the IMPB configuration or use the show ip ip-mac-port-binding violation command to display the entries blocked because of the IMPB check violation.

Example

This example shows how to display all of the entries blocked by the IMPB access control.

```
Switch#show ip ip-mac-port-binding violation
Port            VLAN MAC Address
--------------- ---- -----------------
eth1/0/3        1    01-00-0C-CC-CC-CC
eth1/0/3        1    01-80-C2-00-00-00
eth1/0/4        1    01-00-0C-CC-CC-CD
eth1/0/4        1    01-80-C2-00-00-01

Total Entries: 4

Switch#
```

This example shows how to display the IMPB configuration for all ports.

```
Switch# show ip ip-mac-port-binding

Port           Mode
---------- ------------
eth1/0/1       Strict
eth1/0/2       Strict
eth1/0/3       Loose
eth1/0/4       Loose

Total Entries: 4

Switch#
```

32-4 snmp-server enable traps ip-mac-port-binding

This command is used to enable the sending of SNMP notifications for IMPB. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps ip-mac-port-binding

no snmp-server enable traps ip-mac-port-binding

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of the SNMP notifications for such events. When enabled, the Switch sends violation traps if any violation packet is received.

Example

This example shows how to enable the sending of traps for IMPB.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

33. IP Multicast (IPMC) Commands

33-1 show ip mroute forwarding-cache

This command is used to display the contents in the IP multicast routing forwarding cache database.

show ip mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Parameters

group-addr *GROUP-ADDRESS*	(Optional) Specifies the IP address of the group.
source-addr *SOURCE-ADDRESS*	(Optional) Specifies the IP address of the multicast source.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

The IP multicast forwarding cache is a summary of the IP multicast route table, IGMP snooping group member table, and the multicast router ports.

Example

This example shows how to display the IP multicast routing forwarding cache.

```
Switch#show ip mroute forwarding-cache
(10.1.1.1, 239.0.0.0) VLAN0060
  Outgoing interface list: eth1/0/1, port-channel2

(*,225.0.0.0) VLAN0070
  Outgoing interface list: eth1/0/1-1/0/2

Total entries: 2

Switch#
```

Display Parameters

239.0.0.0	The group address.
10.1.1.1	The source address.
*****	The wildcard source address.
VLAN0060	The interface that multicast data arrived on.
Outgoing interface list	A list of outgoing interfaces for multicast data. It contains Layer 2 switching interfaces.

34. IP Multicast Version 6 (IPMCv6) Commands

34-1 show ipv6 mroute forwarding-cache

This command is used to display the contents in the IPv6 multicast routing forwarding cache database.

show ipv6 mroute forwarding-cache [group-addr *GROUP-ADDRESS* **[source-addr** *SOURCE-ADDRESS***]]**

Parameters

group-addr *GROUP-ADDRESS*	(Optional) Specifies the IPv6 address of the group.
source-addr *SOURCE-ADDRESS*	(Optional) Specifies the IPv6 address of the multicast source.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

The IPv6 multicast forwarding cache is a summary of the IPv6 multicast route table, MLD snooping group member table, and the multicast router ports.

Example

This example shows how to display the IPv6 multicast routing forwarding cache.

```
Switch# show ipv6 mroute forwarding-cache
(2000:60:1:1::10, ff0e::1:1:1) VLAN0060
  Outgoing interface list: eth1/0/1, port-channel2

(2000:60:1:1::10, ff0e::1:1:2) VLAN0060
  Outgoing interface list: eth1/0/1, eth1/0/3

Total entries: 2

Switch#
```

Display Parameters

FF0E::1:1:1	The group address.
2000:60:1:1::10	The source address.
VLAN0060	The interface that multicast data arrived on.
Outgoing interface list	A list of outgoing interfaces for multicast data. It contains Layer 2 switching interfaces.

35. IP Source Guard Commands

35-1 ip verify source vlan dhcp-snooping

This command is used to enable IP source guard for a port. Use the **no** form of this command to disable IP source guard.

ip verify source vlan dhcp-snooping [ip-mac]

no ip verify source vlan dhcp-snooping [ip-mac]

Parameters

ip-mac	(Optional) Specifies to check both IP address and MAC address of the received IP packets.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable the IP source guard on the configured port.

When a port is enabled for IP source guard, the IP packet that arrives at the port will be validated via the port ACL. Port ACL is a hardware mechanism and its entry can come from either a manual configured entry or the DHCP snooping binding database. The packet that fails to pass the validation will be dropped.

There are two types of validations.

- If the **ip-mac** parameter is not specified, the validation is based on the source IP address and VLAN check only.
- If the **ip-mac** parameter is specified, the validation is based on the source MAC address, VLAN and IP address.

Example

This example shows how to enable IP Source Guard on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

35-2 ip source binding

This command is used to create a static entry used for IP source guard. Use the **no** form of this command to delete a static binding entry.

ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

Parameters

MAC-ADDRESS	Specifies the MAC address of the IP-to-MAC address binding entry.
vlan *VLAN-ID*	Specifies the VLAN that the valid host belongs to.
IP-ADDRESS	Specifies the IP address of the IP-to-MAC address binding entry.
Interface *INTERFACE-ID*	Specifies the interfaces that the valid host is connected. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to add or delete a static binding entry used for IP source guard checking. The parameters specified for the command must exactly match the entry to be deleted.

If the MAC address and the VLAN for the configured entry already exist, the existing binding entry is updated.

Example

This example shows how to configure an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch# configure terminal
Switch(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

This example shows how to delete an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

35-3 show ip source binding

This command is used to display an IP-source guard binding entry.

show ip source binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [dhcp-snooping | static] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID* **[, | -]]**

Parameters

IP-ADDRESS	(Optional) Specifies to display the IP-source guard binding entry based on IP address.

MAC-ADDRESS	(Optional) Specifies to display the IP-source guard binding entry based on MAC address.
dhcp-snooping	(Optional) Specifies to display the IP-source guard binding entry learned by DHCP binding snooping.
static	(Optional) Specifies to display the IP-source guard binding entry that is manually configured.
vlan *VLAN-ID*	(Optional) Specifies to display the IP-source guard binding entry based on VLAN.
Interface *INTERFACE-ID*	(Optional) Specifies to display the IP-source guard binding entry based on ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

IP source guard binding entries are either manually configured or automatically learned by DHCP snooping to guard IP traffic.

Example

This example shows how to display all IP Source Guard binding entries.

```
Switch#show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN Interface
----------------- --------------- ---------- ------------- ---- ---------
00-01-01-01-01-10 10.1.1.11       infinite   static        1    eth1/0/3
00-01-02-03-04-05 10.1.1.1        infinite   static        2    eth1/0/10

Total Entries: 2

Switch#
```

Display Parameters

MAC Address	The client's hardware MAC address.
IP Address	The client's IP address assigned from the DHCP server or configured by the user.
Lease (sec)	The IP address lease time.
Type	The binding type. Static bindings are configured manually. Dynamic binding are learned from DHCP snooping.
VLAN	The VLAN number of the client interface.
Interface	The interface that connects to the DHCP client host.

35-4 show ip verify source

This command is used to display the hardware port ACL entry on a particular interface.

show ip verify source [interface *INTERFACE-ID* **[, | -]]**

Parameters

Interface *INTERFACE-ID*	(Optional) Specifies a port or range of ports to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the hardware port ACL entries for a port in the hardware table. It indicates the hardware filter behavior that IP source guard is verified upon.

Example

This example shows how to display when DHCP snooping is enabled on VLANs 100 to 110, the interface with IP source filter mode that is configured as IP, and that there is an existing IP address binding 10.1.1.1 on VLAN 100.

```
Switch# show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip          active      10.1.1.1        -                 100
eth1/0/3        ip          active      deny-all        -                 101-120

Total Entries: 2

Switch#
```

This example shows how to display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC that binds IP address 10.1.1.10 to MAC address 00-01-01-01-01-01 on VLAN 100 and IP address 10.1.1.11 to MAC address 00-01-01-01-01-10 on VLAN 101.

```
Switch# show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip-mac      active      10.1.1.10       00-01-01-01-01-01 100
eth1/0/3        ip-mac      active      10.1.1.11       00-01-01-01-01-10 101
eth1/0/3        ip-mac      active      deny-all        -                 102-120

Total Entries: 3

Switch#
```

Display Parameters

Interface	The interface that has IP inspection enabled.
Filter-type	The type of IP Source Guard in operation. • **ip** - Just use an IP address to authorize IP packets. • **ip-mac** - Use the IP and MAC address to authorize IP packets.
Filter-Mode	• **active** - Actively verify IP source entries. • **inactive-trust-port** - Enable DHCP snooping to trust ports with no IP source entry verification active. • **inactive-no-snooping-vlan** - No DHCP snooping VLAN configured with no IP source entry verification active.
IP address	The client's IP address assigned from the DHCP server or configured by the user.
MAC address	The client's MAC address.
VLAN	The VLAN number of the client interface.

36. IP Utility Commands

36-1 ping

This command is used to diagnose basic network connectivity.

ping {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [count** *TIMES***] [timeout** *SECONDS***] [source {***IP-ADDRESS* **|** *IPV6-ADDRESS***}]**

Parameters

ip	(Optional) Specifies the destination IPv4 address.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
ipv6	(Optional) Specifies the destination IPv6 address.
IPV6-ADDRESS	Specifies the IPv6 address of the system to discover.
HOST-NAME	Specifies the host name of the system to discover.
count *TIMES*	(Optional) Specifies to stop after sending the specified number of echo request packets.
timeout *SECONDS*	(Optional) Specifies response timeout value in seconds.
source {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**	Specifies the source IP address used for the ping packet. The specified IP address must one of the IP address configured for the Switch. The destination address and the source IP must be the same type of address, both are IPv4 or IPv6.

Default

The **count** value is disabled. The ping will continue until the user terminates the process.

The **timeout** value is 1 second.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to verify the reachability, reliability, and delay of the path to the destination host.

To terminate the ping before it has finished, press CTRL+C.

Example

This example shows how to ping the host with IP address 211.21.180.1 with count 4 times.

```
Switch# ping 211.21.180.1 count 4

Reply from 211.21.180.1, time=10ms
Reply from 211.21.180.1, time<10ms
Reply from 211.21.180.1, time<10ms
Reply from 211.21.180.1, time<10ms

 Ping Statistics for 211.21.180.1
 Packets: Sent =4, Received =4, Lost =0


Switch#
```

This example shows how to ping the host with IPv6 address 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch# ping 2001:238:f8a:77:7c10:41c0:6ddd:ecab

Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms
Reply from 2001:238:f8a:77:7c10:41c0:6ddd:ecab , bytes=100, time<10 ms

 Ping Statistics for 2001:238:f8a:77:7c10:41c0:6ddd:ecab
 Packets: Sent =4, Received =4, Lost =0

Switch#
```

36-2 ping access-class

This command is used to specify an access list to restrict access via ping. Use the **no** command to remove the access list check.

ping access-class *IP-ACL*

no ping access-class *IP-ACL*

Parameters

IP-ACL	Specifies a standard IP access list. The source address field of the permit or deny entry defines the valid or invalid host. To permit access via ping, specify the source address field and 'any' in the destination address field of the access list if the field is present.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify an access list to restrict access via ping. The specified access list does not need to exist to execute the command.

Example

This example shows how to create a ping access-class which is used to restrict the ping only from the host 220.1.1.1 via a standard IP access list.

```
Switch# configure terminal
Switch(config)# ip access-list ping-filter
Switch(config-ip-acl)# permit 220.1.1.1 255.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# ping access-class ping-filter
Switch(config)#
```

37. IPv6 Snooping Commands

37-1 ipv6 snooping policy

This command is used to create or modify an IPv6 snooping policy. This command will enter the IPv6 snooping configuration mode. Use the **no** form of this command to delete an IPv6 snooping policy.

ipv6 snooping policy *POLICY-NAME*

no ipv6 snooping policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the name of the snooping policy.

Default

No IPv6 snooping policy is created.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create an IPv6 snooping policy. After an IPv6 snooping policy has been created, use the **ipv6 snooping attach-policy** command to apply the policy on a specific interface.

Example

This example shows how to create an IPv6 snooping policy named policy1.

```
Switch# configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#
```

37-2 protocol

This command is used to specify that addresses should be snooped with DHCPv6 or NDP. Use the **no** form of this command to indicate that a protocol will not to be used for snooping.

protocol {dhcp | ndp}

no protocol {dhcp | ndp}

Parameters

dhcp	Specifies that addresses should be snooped in DHCPv6 packets.
ndp	Specifies that addresses should be snooped in NDP packets.

Default

By default, both DHCPv6 and ND snooping are disabled.

Command Mode

IPv6 Snooping Configuration Mode.

Usage Guideline

ND Snooping is designed for a stateless auto-configuration assigned IPv6 address and manually configured IPv6 address. Before assigning an IPv6 address, the host must perform Duplicate Address Detection first. ND snooping detects DAD messages (DAD NS and DAD NA) to build its binding database. The NDP packet (NS and NA) is also used to detect whether a host is still reachable and determine whether to delete a binding or not.

DHCPv6 Snooping sniffs the DHCPv6 packets sent between the DHCPv6 client and server in the address assigning procedure. When a DHCPv6 client successfully got a valid IPv6 address, DHCPv6 snooping creates its binding database.

Example

This example shows how to enable DHCPv6 snooping.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# protocol dhcp
Switch(config-ipv6-snooping)#
```

37-3 limit address-count

This command is used to limit the maximum number of IPv6 snooping binding entries. Use the **no** form of this command to revert to the default setting.

limit address-count *MAXIMUM*

no limit address-count

Parameters

MAXIMUM	Specifies the maximum number of IPv6 snooping binding entries. The range is from 0 to 511.

Default

By default, there is no limit configured.

Command Mode

IPv6 Snooping Configuration Mode.

Usage Guideline

Use this command to limit the number of IPv6 binding entries on which the IPv6 snooping policy is applied. This command helps to limit the binding table size.

Example

This example shows how to limit the number of IPv6 snooping binding entries to 25.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 25
Switch(config-ipv6-snooping)#
```

37-4 ipv6 snooping attach-policy

This command is used to apply an IPv6 snooping policy to a specified VLAN. Use the no form of this command to remove the binding.

ipv6 snooping policy attach-policy *POLICY-NAME*

no ipv6 snooping policy attach-policy

Parameters

POLICY-NAME	Specifies the name of the snooping policy.

Default

None.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to apply the policy on a specific VLAN after an IPv6 snooping policy has been created.

Example

This example shows how to enable IPv6 snooping on VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 snooping policy policy1
Switch(config-ipv6-snooping)# limit address-count 100
Switch(config-ipv6-snooping)# exit
Switch(config)# vlan 200
Switch(config-vlan)# ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

37-5 ipv6 snooping station-move deny

This command is used to deny the station move function for IPv6 snooping entries. Use the **no** form of this command to revert to the default setting.

ipv6 snooping station-move deny

no ipv6 snooping station-move deny

Parameters

None.

Default

IPv6 snooping is permitting station moves.

Command Mode

Global Configuration Mode.

Usage Guideline

When station move is permitted, the dynamic snooping binding entry with same VLAN ID and MAC address on the specific port can move to another port if it detects the following conditions:

- A DHCPv6 snooping binding entry starts a new DHCP process on a new interface.
- An ND snooping binding entry starts a new DAD process on a new interface.

Example

This example shows how to deny the station move function.

```
Switch# configure terminal
Switch(config)# ipv6 snooping station-move deny
Switch(config)#
```

37-6 show ipv6 snooping policy

This command is used to display DHCPv6 guard information.

show ipv6 snooping policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the DHCPv6 guard policy name.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display DHCPv6 guard information. If no parameter is specified, information of all policies will be displayed.

Example

This example shows how to display DHCPv6 guard information.

```
Switch#show ipv6 snooping policy

Snooping policy: policy1
    Protocol: DHCP
    Limit Address Count: 25
    Target VLAN: 200

Switch#
```

38. IPv6 Source Guard Commands

38-1 ipv6 source binding vlan

This command is used to add a static entry to the binding table. Use the **no** form of this command to remove the static binding entry.

ipv6 source binding *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

no ipv6 source binding *MAC-ADDRESS* **vlan** *VLAN-ID IPV6-ADDRESS* **interface** *INTERFACE-ID*

Parameters

MAC-ADDRESS	Specifies the MAC address of the manual binding entry.
vlan *VLAN-ID*	Specifies the binding VLAN of the manual binding entry.
IPV6-ADDRESS	Specifies the IPv6 address of the manual binding entry.
interface *INTERFACE-ID*	Specifies the interface number of the manual binding entry.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to set the static manual binding entry of the binding table.

Example

This example shows how to configure an IPv6 Source Guard entry with the IPv6 address of 2000::1 and MAC address of 00-01-02-03-04-05 at VLAN 2 on port 1.

```
Switch# configure terminal
Switch(config)# ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface eth1/0/1
Switch(config)#
```

38-2 ipv6 source-guard policy

This command is used to create an IPv6 source guard policy and enter into the Source-guard Policy Configuration Mode. Use the **no** form of this command to remove an IPv6 source guard policy.

ipv6 source-guard policy *POLICY-NAME*

no ipv6 source-guard policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the name of the source guard policy.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create or remove a source guard policy name. This command will enter into the Source-guard Policy Configuration Mode.

Example

This example shows how to create an IPv6 source guard policy.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

38-3 deny global-autoconfig

This command is used to deny auto-configured traffic. Use the **no** form of this command to disable this function.

deny global-autoconfig

no deny global-autoconfig

Parameters

None.

Default

By default, this option is permitted.

Command Mode

Source-guard Policy Configuration Mode.

Usage Guideline

Use this command to deny data traffic from auto-configured global address. It is useful when all global addresses on a link are assigned by DHCP and the administrator that wants to block hosts with self-configured addresses from sending traffic.

Example

This example shows how to deny auto-configured traffic.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# deny global-autoconfig
Switch(config-source-guard)#
```

38-4 permit link-local

This command is used to allow hardware permitted data traffic send by the link-local address. Use the **no** form of this command to disable this function

permit link-local

no permit link-local

Parameters

None.

Default

By default, this option is denied.

Command Mode

Source-guard Policy Configuration Mode.

Usage Guideline

Use this command to enable or disable hardware to permit data traffic sent by the link-local address.

Example

This example shows how to allow all data traffic that is send by the link-local address.

```
Switch# configure terminal
Switch(config)# ipv6 source-guard policy policy1
Switch(config-source-guard)# permit link-local
Switch(config-source-guard)#
```

38-5 ipv6 source-guard attach-policy

This command is used to apply IPv6 source guard on an interface. Use the **no** form of this command to remove the source guard from the interface.

ipv6 source-guard attach-policy [*POLICY-NAME***]**

no ipv6 source-guard attach-policy

Parameters

POLICY-NAME	(Optional) Specifies the name of the source guard policy.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

When the command is applied to a port, the received IPv6 packet except ND, RA, RS and DHCP messages will perform the address binding check. The packet is allowed when it matches any of the address binding table's entries. The binding table includes the dynamic table (created by IPv6 snooping) and the static table (created by the **ipv6 source binding vlan** command)

If the policy name is not specified, the default source guard policy will permit packets sent by the auto-configured address and deny packets sent by the link-local address.

Example

This example shows how to apply the IPv6 source guard policy “pol1” to port 3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

38-6 show ipv6 source-guard policy

This command is used to display the IPv6 source guard policy configuration.

show ipv6 source-guard policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the source guard policy.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the IPv6 source guard policy configuration. If no parameter is specified, all IPv6 source guard polices will be display.

Example

This example shows how to display the IPv6 source guard policy configuration.

```
Switch# show ipv6 source-guard policy

Policy Test configuration:
    permit link-local
    deny global-autoconf
    Target: eth1/0/3

Switch#
```

38-7 show ipv6 neighbor binding

This command is used to display the IPv6 binding table.

show ipv6 neighbor binding [vlan *VLAN-ID***] [interface** *INTERFACE-ID***] [ipv6** *IPV6-ADDRESS***] [mac** *MAC-ADDRESS***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies to displays the binding entries that match the specified VLAN.
interface *INTERFACE-ID*	(Optional) Specifies to displays the binding entries that match the specified interface number.
ipv6 *IPV6-ADDRESS*	(Optional) Specifies to displays the binding entries that match the specified IPv6 address.
mac *MAC-ADDRESS*	(Optional) Specifies to displays the binding entries that match the specified MAC address.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the entries of the binding table.

Example

This example shows how to display the entries of the binding table.

```
Switch#
show ipv6 neighbor binding

Codes: D - DHCPv6 Snooping, S - Static, N - ND Snooping
  IPv6 address                  MAC address    Interface       VLAN Time left
N FE80::A8BB:CCFF:FE01:F500     AABB.CC01.F500 eth1/0/1        100  8850
S FE80::21D:71FF:FE99:4900      001D.7199.4900 eth1/0/1        100  N/A
N 2001:600::1                   AABB.CC01.F500 eth1/0/2        100  3181
D 2001:300::1                   AABB.CC01.F500 Port-channel3   100  9559
D 2001:100::2                   AABB.CC01.F600 eth1/0/1        200  9196
D 2001:400::1                   001D.7199.4900 eth1/0/2        100  1568
S 2001:500::1                   000A.000B.000C eth1/0/13       300  N/A

Total Entries: 7

Switch#
```

Display Parameters

Codes	The codes for the IPv6 snooping owner. • **D** - DHCPv6 Snooping. • **S** - Static. • **N** - ND Snooping.
IPv6 address	The IPv6 address of the binding entry.
MAC address	The MAC address of the binding entry.

Interface	The interface number of the binding entry.
VLAN	The VLAN of the binding entry.
Time left	The rest time for aging the binding entry. It is the inactivity for the static binding entry.

39. Link Aggregation Control Protocol (LACP) Commands

39-1 channel-group

This command is used to assign an interface to a channel group. Use the **no** form of this command to remove an interface from a channel-group.

channel-group *CHANNEL-NO* **mode {on | active | passive}**

no channel-group

Parameters

CHANNEL-NO	Specifies the channel group ID. The valid range is 1 to 32.
on	Specifies that the interface is a static member of the channel-group.
active	Specifies the interface to operate in LACP active mode.
passive	Specifies the interface to operate in LACP passive mode.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.

If the **on** parameter is specified, the channel group type is static. If the **active** or **passive** parameter is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

Use the **no** form of this command to remove the interface from the channel group. If the channel group has no member ports left after a port is removed, the channel group will be deleted automatically. A port channel can also be removed by using the **no interface port-channel** command.

If the security function is enabled on a port, this port cannot be specified as a channel group member.

Example

This example shows how to assign ports 4 and 5 to a new LACP channel-group, with an ID of 3, and sets the LACP mode to active.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

39-2 lacp port-priority

This command is used to configure the port priority. Use the **no** form of this command to revert the port priority to the default settings.

lacp port-priority *PRIORITY*

no lacp port-priority

Parameters

PRIORITY	Specifies the port priority. The range is 1 to 65535.

Default

The default port-priority is 32768.

Command Mode

Interface Configuration Mode.

Usage Guideline

The LACP port-priority determines which ports can join a port-channel and which ports are put in the standalone mode. The lower value has a higher priority. If two or more ports have the same priority, the port number determines the priority.

Example

This example shows how to configure the port priority to 20000 on ports 4 and 5.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-1/0/5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

39-3 lacp timeout

This command is used to configure the LACP long or short timer. Use the **no** form of this command to revert to the default setting.

lacp timeout {short | long}

no lacp timeout

Parameters

short	Specifies that there will be 3 seconds before invalidating received LACPDU information. Once the partner recognizes this information in the received PDU, LACP PDU periodic transmissions will be sent at 1 second intervals.
long	Specifies that there will be 90 seconds before invalidating received LACPDU information. Once the partner recognizes this information in the received PDU, LACP PDU periodic transmissions will be sent at 30 second intervals.

Default

By default, the LACP timeout mode is short.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Example

This example shows how to configure the port LACP timeout to long mode on port 1.

```
Switch# configure terminal
Switch(config)# interface  eth1/0/1
Switch(config-if)# lacp timeout long
Switch(config-if)#
```

39-4 lacp system-priority

This command is used to configure the system priority. Use the **no** form of this command to revert to the default setting.

lacp system-priority *PRIORITY*

no lacp system-priority

Parameters

PRIORITY	Specifies the system priority. The range is 1 to 65535.

Default

The default LACP system-priority is 32768.

Command Mode

Global Configuration Mode.

Usage Guideline

During LACP negotiation, the system priority and port priority of the local partner will be exchanged with the remote partner. When the maximum number of actual members exceeds the limitation, the Switch will use port priority to determine whether a port is operating in a backup mode or in an active mode. The LACP system-priority determines the Switch that controls the port priority. Port priorities on the other switch are ignored.

The lower value has a higher priority. If two switches have the same system priority, the LACP system ID (MAC) determines the priority. The LACP system priority command applies to all LACP port-channels on the Switch.

Example

This example shows how to configure the LACP system priority to be 30000.

```
Switch# configure terminal
Switch(config)# lacp system-priority 30000
Switch(config)#
```

39-5 port-channel load-balance

This command is used to configure the load balance algorithm that the Switch uses to distribute packets across ports in the same channel. Use the **no** form of this command to revert to the default setting.

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac}

no port-channel load-balance

Parameters

dst-ip	Specifies that the Switch should examine the IP destination address.
dst-mac	Specifies that the Switch should examine the MAC destination address.
src-dst-ip	Specifies that the Switch should examine the IP source address and IP destination address.
src-dst-mac	Specifies that the Switch should examine the MAC source and MAC destination address.
src-ip	Specifies that the Switch should examine the IP source address.
src-mac	Specifies that the Switch should examine the MAC source address.

Default

The default load balance algorithm is **src-dst-mac**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the load balance algorithm. Only one algorithm can be specified.

Example

This example shows how to configure the load balance algorithm as **src-ip**.

```
Switch# configure terminal
Switch(config)# port-channel load-balance src-ip
Switch(config)#
```

39-6 show channel-group

This command is used to display the channel group information.

show channel-group [channel [*CHANNEL-NO*] {detail | neighbor} | load-balance | sys-id]

Parameters

channel	(Optional) Specifies to display information for the specified port-channels.
CHANNEL-NO	(Optional) Specifies the channel group ID.
detail	(Optional) Specifies to display detailed channel group information.
neighbor	(Optional) Specifies to display neighbor information.
load-balance	(Optional) Specifies to display the load balance information.
sys-id	(Optional) Specifies to display the system identifier that is being used by LACP.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no port-channel number is specified, all port channels will be displayed. If no parameter is specified with the **show channel-group** command, the summary information of the channel group will be displayed.

Example

This example shows how to display the detailed information of all port-channels.

```
Switch# show channel-group channel detail

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode
LACP state:
  bndl:     Port is attached to an aggregator and bundled with other ports.
  hot-sby:  Port is in a hot-standby state.
  indep:    Port is in an independent state(not bundled but able to switch data
            traffic)
  down:     Port is down.

Channel Group 1
  Member Ports: 2, Maxports = 8, Protocol: LACP
  Description:
                        LACP         Port       Port
  Port          Flags   State        Priority   Number
  ------------------------------------------------------
  eth1/0/10     SA      bndl         32768      10
  eth1/0/11     SA      bndl         32768      11

Channel Group 2
  Member Ports: 2, Maxports = 8, Protocol: Static
                        LACP         Port       Port
  Port          Flags   State        Priority   Number
  ------------------------------------------------------
  eth1/0/8      N/A     bndl         N/A        N/A
  eth1/0/9      N/A     down         N/A        N/A

Switch#
```

This example shows how to display the neighbor information for port channel 3.

```
Switch# show channel-group channel 3 neighbor

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3
               Partner                  Partner   Partner   Partner
  Port         System ID                PortNo    Flags     Port_Pri
  -----------------------------------------------------------------
  eth1/0/1     32768,F8-E9-80-1F-23-90   12        SP        32768
  eth1/0/2     32768,F8-E9-80-1F-23-90   13        SP        32768

Switch#
```

This example shows how to display the load balance information for all channel groups.

```
Switch# show channel-group load-balance

load-balance algorithm: src-dst-mac

Switch#
```

This example shows how to display the system identifier information.

```
Switch# show channel-group sys-id

System-ID: 32765,00-02-4B-29-3A-00

Switch#
```

This example shows how to display the summary information for all port-channels.

```
Switch# show channel-group

load-balance algorithm: src-dst-mac
System-ID: 32768,3C-1E-04-A1-CC-00

Group          Protocol
-----------------------
1              LACP
2              Static

Switch#
```

40. Link Layer Discovery Protocol (LLDP) Commands

40-1 clear lldp counters

This command is used to delete LLDP statistics.

clear lldp counters [all | interface *INTERFACE-ID* **[, | -]]**

Parameters

all	(Optional) Specifies to clear LLDP counter information for all interfaces and global LLDP statistics.
interface *INTERFACE-ID*	(Optional) Specifies the interface to clear LLDP counter information.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command with the **interface** parameter to reset LLDP statistics of the specified interface(s). Use this command with the **all** parameter to clear global LLDP statistics and the LLDP statistics on all interfaces. If no parameter is specified, only the LLDP global counters will be cleared.

Example

This example shows how to clear all LLDP statistics.

```
Switch# clear lldp counters all
Switch#
```

40-2 clear lldp table

This command is used to delete LLDP information learned from neighboring devices.

clear lldp table {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear LLDP neighboring information for all interfaces.
interface *INTERFACE-ID*	Specifies the interfaces to be cleared.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command with the **interface** parameter to clear information learned from neighboring devices on the specified interface(s). Use this command with the **all** parameter to clear all information learned from neighboring devices.

Example

This example shows how to clear all neighboring information on all interfaces.

```
Switch# clear lldp table all
Switch#
```

40-3 lldp dot1-tlv-select

This command is used to specify which optional type-length-value settings (TLVs) in the IEEE 802.1 Organizationally Specific TLV set will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of TLVs.

lldp dot1-tlv-select {port-vlan | vlan-name [*VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

no lldp dot1-tlv-select {port-vlan | vlan-name [*VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

Parameters

port-vlan	Specifies the port VLAN ID TLV to send. The Port VLAN ID TLV is an optional fixed length TLV that allows a VLAN bridge port to advertise the port VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
vlan-name	Specifies the VLAN name TLV to send. The VLAN name TLV is an optional TLV that allows an IEEE 802.1Q-compatible IEEE 802 LAN station to advertise the assigned name of any VLAN with which it is configured.
VLAN-ID	Specifies the ID of the VLAN in the VLAN name TLV. The VLAN ID range is 1 to 4094. If no VLAN ID is specified, all configured VLANs for the VLAN name TLV will be cleared and no VLAN name TLV will be sent.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
protocol-identity	Specifies the Protocol Identity TLV to send. The Protocol Identity TLV is an optional TLV that allows an IEEE 802 LAN station to advertise particular protocols that are accessible through the port.
PROTOCOL-NAME	(Optional) Specifies the protocol name here. The valid strings for PROTOCOL-NAME are: • **eapol** - Extensible Authentication Protocol (EAP) over LAN

- **lacp** - Link Aggregation Control Protocol
- **stp** - Spanning Tree Protocol

Default

No IEEE 802.1 Organizationally Specific TLV is selected.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration. If the optional TLVs advertisement state is enabled, they will be encapsulated in LLDPDUs and sent to other devices.

The protocol identity TLV optional data type indicates whether to advertise the corresponding local system's protocol identity instance on the port. The protocol identity TLV provides a way for devices to advertise protocols that are important to the operation of the network. For example, protocols like Spanning Tree Protocol, Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. When both of the protocol functions are working and the protocol identity is enabled for advertising on a port, the protocol identity TLV will be advertised.

Only when the interface is a member port of the configured VLAN ID, the VLAN will be advertised in VLAN Name TLV.

Example

This example shows how to enable advertising Port VLAN ID TLV.

```
Switch#configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

This example shows how to enable the VLAN Name TLV advertisement from vlan1 to vlan3.

```
Switch# configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

This example shows how to enable the LACP Protocol Identity TLV advertisement.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-identity lacp
Switch(config-if)#
```

40-4 lldp dot3-tlv-select

This command is used to specify which optional TLVs in the IEEE 802.3 Organizationally Specific TLV set will encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size]

no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size]

Parameters

mac-phy-cfg	(Optional) Specifies the MAC/PHY Configuration/Status TLV to send. The MAC/PHY Configuration/Status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
link-aggregation	(Optional) Specifies the Link Aggregation TLV to send. The Link Aggregation TLV indicates contains the following information. Whether the link is capable of being aggregated, whether the link is currently in an aggregation, and the aggregated port channel ID of the port. If the port is not aggregated, then the ID is 0.
max-frame-size	(Optional) Specifies the Maximum Frame Size TLV to send. The Maximum Frame Size TLV indicates the maximum frame size capability of the implemented MAC and PHY.

Default

No IEEE 802.3 Organizationally Specific TLV is selected.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to enable the advertisement of the optional IEEE 802.3 Organizationally Specific TLVs. The respective TLV will be encapsulated in LLDPDU and sent to other devices if the advertisement state is enabled.

Example

This example shows how to enable the advertising MAC/PHY Configuration/Status TLV.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

40-5 lldp fast-count

This command is used to configure the LLDP-MED fast start repeat count option on the Switch. Use the **no** form of this command to revert to the default setting.

lldp fast-count *VALUE*

no lldp fast-count

Parameters

VALUE	Specifies the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Default

By default, this value is 4.

Command Mode

Global Configuration Mode.

Usage Guideline

When an LLDP-MED Capabilities TLV is detected, the application layer will start the fast start mechanism. This command is used to configure the fast start repeat count which indicates the number of LLDP message transmissions for one complete fast start interval.

Example

This example shows how to configure the LLDP MED fast start repeat count.

```
Switch# configure terminal
Switch(config)# lldp fast-count 10
Switch(config)#
```

40-6 lldp hold-multiplier

This command is used to configure the hold multiplier for LLDP updates on the Switch. Use the **no** form of this command to revert to the default setting.

lldp hold-multiplier *VALUE*

no hold-multiplier

Parameters

VALUE	Specifies the multiplier on the LLDPDUs transmission interval that used to compute the TTL value of an LLDPDU. This value must be between 2 and 10.

Default

By default, this value is 4.

Command Mode

Global Configuration Mode.

Usage Guideline

This parameter is a multiplier on the LLDPDUs transmission interval that is used to compute the TTL value in an LLDPDU. The lifetime is determined by the hold-multiplier times the TX-interval. At the partner switch, when the TTL for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.

Example

This example shows how to configure the LLDP hold-multiplier to 3.

```
Switch# configure terminal
Switch(config)# lldp hold-multiplier 3
Switch(config)#
```

40-7 lldp management-address

This command is used to configure the management address that will be advertised on the physical interface. Use the **no** form of this command to remove the settings.

lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

no lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Parameters

IP-ADDRESS	(Optional) Specifies the IPv4 address that is carried in the management address TLV.
IPV6-ADDRESS	(Optional) Specifies the IPv6 address that is carried in the management address TLV.

Default

No LLDP management address is configured (no Management Address TLV is sent).

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration. This command specifies the IPv4/IPv6 address that is carried in the management address TLV on the specified port. If an IP address is specified, but the address is not one of the addresses of the system interfaces, the address will not be sent.

If no parameter is specified, the Switch will find least one IPv4 and IPv6 address of the VLAN with the smallest VLAN ID. If no applicable IPv4/IPv6 address exists, no management address TLV will be advertised. Once the administrator configures an address, both of the default IPv4 and IPv6 management address will become inactive and won't be sent. The default IPv4 or IPv6 address will be active again when all the configured addresses are removed. Multiple IPv4/IPv6 management addresses can be configured by using this command multiple times.

Use the **no lldp management-address** command without a management address to disable the management address adverted in LLDPDUs. If there is no effective management address in the list, no Management Address TLV will be sent.

Example

This example shows how to configure the management IPv4 address on ports 1 to 3.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-3
Switch(config-if-range)# lldp management-address 10.1.1.1
Switch(config-if-range)#
```

This example shows how to configure the management IPv6 address on ports 4 to 6.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-6
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

This example shows how to remove the management IPv4 address from ports 1 to 3.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/1-3
Switch(config-if-range)# no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

This example shows how to remove the management IPv6 address from ports 4 to 6.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-6
Switch(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

This example shows how to remove all management IPv4/IPv6 addresses from port 5. No management address TLV will be sent from port 5.

```
Switch# configure terminal
Switch(config)# interface eth1/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

40-8 lldp med-tlv-select

This command is used to specify which optional LLDP-MED TLV will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

lldp med-tlv-select [capabilities | inventory-management | network-policy]

no lldp med-tlv-select [capabilities | inventory-management | network-policy]

Parameters

capabilities	(Optional) Specifies to transmit the LLDP-MED capabilities TLV.
inventory-management	(Optional) Specifies to transmit the LLDP-MED inventory management TLV.
network-policy	(Optional) Specifies to transmit the LLDP-MED network policy TLV.

Default

No LLDP-MED TLV is selected.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to enable or disable transmitting LLDP-MED TLVs. When disabling the transmission of the Capabilities TLV, LLDP-MED on the physical interface will be disabled at the same time. In other words, all LLDP-MED TLVs will not be sent, even when other LLDP-MED TLVs are enabled to transmit.

By default, the Switch only sends LLDP packets until it receives LLDP-MED packets from the end device. The Switch continues to send LLDP-MED packets until it only receives LLDP packets.

Example

This example shows how to enable transmitting LLDP-MED TLVs and LLDP-MED Capabilities TLVs.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp med-tlv-select capabilities
Switch(config-if)#
```

40-9 lldp receive

This command is used to enable a physical interface to receive LLDP messages. Use the **no** form of this command to disable receiving LLDP messages.

lldp receive

no lldp receive

Parameters

None.

Default

LLDP is enabled on all supported interfaces.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to enable a physical interface to receive LLDP messages. When LLDP is not running, the Switch does not receive LLDP messages.

Example

This example shows how to enable a physical interface to receive LLDP messages.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp receive
Switch(config-if)#
```

40-10 lldp reinit

This command is used to configure the minimum time of re-initialization the delay interval on the Switch. Use the **no** form of this command to revert to the default setting.

lldp reinit *SECONDS*

no lldp reinit

Parameters

SECONDS	Specifies the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

A re-enabled LLDP physical interface will wait for the re-initialization delay after the last disable command before reinitializing.

Example

This example shows how to configure the re-initialization delay interval to 5 seconds.

```
Switch# configure terminal
Switch(config)# lldp reinit 5
Switch(config)#
```

40-11 lldp run

This command is used to enable LLDP globally. Use the **no** form of this command to revert to the default setting.

lldp run

no lldp run

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to globally enable LLDP and then the Switch can start to transmit LLDP packets and receive and process the LLDP packets. However, the transmission and receiving of LLDP can be controlled respectively by the **lldp transmit** command and the **lldp receive** command in the interface configuration mode. LLDP takes effect on a physical interface only when it is enabled both globally and on the physical interface.

By advertising LLDP packets, the Switch announces the information to its neighbor through physical interfaces. On the other hand, the Switch will learn the connectivity and management information from the LLDP packets advertised from the neighbor(s).

Example

This example shows how to enable LLDP.

```
Switch# configure terminal
Switch(config)# lldp run
Switch(config)#
```

40-12 lldp forward

This command is used to enable the LLDP forwarding state. Use the **no** form of this command to revert to the default settings.

lldp forward

no lldp forward

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

This is a global control for the LLDP forward. When the LLDP global state is disabled and LLDP forwarding is enabled, the received LLDPDU packet will be forwarded.

Example

This example shows how to enable the LLDP global forwarding state.

```
Switch# configure terminal
Switch(config)# lldp forward
Switch(config)#
```

40-13 lldp tlv-select

This command is used to select the TLVs in the 802.1AB basic management set, will be transmitted and encapsulated in the LLDPDUs, and sent to neighbor devices. Use the **no** form of this command to disable this option.

lldp tlv-select [port-description | system-capabilities | system-description | system-name]

no lldp tlv-select [port-description | system-capabilities | system-description | system-name]

Parameters

port-description	(Optional) Specifies the port description TLV to send. The port description TLV allows network management to advertise the IEEE 802 LAN station's port description.

system-capabilities	(Optional) Specifies the system capabilities TLV to send. The system capabilities field will contain a bit-map of the capabilities that defines the primary functions of the system.
system-description	(Optional) Specifies the system description TLV to send. The system description should include the full name and version identification of the system's hardware type, software operating system, and networking software.
system-name	(Optional) Specifies the system name TLV to send. The system name should be the system's fully qualified domain name.

Default

No optional 802.1AB basic management TLV is selected.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to select the optional TLVs to be transmitted. If the optional TLVs advertisement is selected, they will be encapsulated in the LLDPDU and sent to other devices.

Example

This example shows how to enable all supported optional 802.1AB basic management TLVs.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp tlv-select
Switch(config-if)#
```

This example shows how to enable advertising the system name TLV.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp tlv-select system-name
Switch(config-if)#
```

40-14 lldp transmit

This command is used to enable the LLDP advertise (transmit) capability. Use the **no** form of this command to disable LLDP transmission.

lldp transmit

no lldp transmit

Parameters

None.

Default

By default, LLDP transmit is enabled on all supported interfaces.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to enable LLDP transmission on a physical interface. When LLDP is not running, the Switch does not transmit LLDP messages.

Example

This example shows how to enable LLDP transmission.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)#
```

40-15 lldp tx-delay

This command is used to configure the transmission delay timer. This delay timer defines the minimum interval between the sending of LLDP messages due to constantly changing MIB content. Use the **no** form of this command to revert to the default setting.

lldp tx-delay *SECONDS*

no lldp tx-delay

Parameters

SECONDS	Specifies the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

The LLDP transmission interval must be greater than or equal to four times of the transmission delay timer.

Example

This example shows how to configure the transmission delay timer to 8 seconds.

```
Switch# configure terminal
Switch(config)# lldp tx-delay 8
Switch(config)#
```

40-16 lldp tx-interval

This command is used to configure the LLDPDUs transmission interval on the Switch. Use the **no** form of this command to revert to the default setting.

lldp tx-interval *SECONDS*

no lldp tx-interval

Parameters

SECONDS	Specifies the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.

Default

By default, this value is 30 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

This interval controls the rate at which LLDP packets are sent.

Example

This example shows how to configure that LLDP updates are sent every 50 seconds.

```
Switch# configure terminal
Switch(config)# lldp tx-interval 50
Switch(config)#
```

40-17 snmp-server enable traps lldp

This command is used to enable the sending of SNMP notifications for LLDP and LLDP-MED. Use the **no** form of this command disable this feature.

snmp-server enable traps lldp [med]

no snmp-server enable traps lldp [med]

Parameters

med	(Optional) Specifies to enable the LLDP-MED trap state.

Default

The LLDP and LLDP-MED trap states are disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use the **snmp-server enable traps lldp** command to enable the sending of LLDP notifications.

Use the **snmp-server enable traps lldp med** command to enable the sending of LLDP-MED notifications.

Example

This example shows how to enable the LLDP MED trap.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps lldp med
Switch(config)#
```

40-18 lldp notification enable

This command is used to enable the sending of LLDP and LLDP-MED notifications for the interface. Use the **no** form of this command to disable the sending.

lldp [med] notification enable

no lldp [med] notification enable

Parameters

med	(Optional) Specifies to enable the LLDP-MED notification state.

Default

The LLDP and LLDP-MED notification states are disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use the **lldp notification enable** command to enable the sending of LLDP notifications.

Use the **lldp med notification enable** command to enable the sending of LLDP-MED notifications.

Example

This example shows how to enable the sending of LLDP-MED notifications from port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# lldp med notification enable
Switch(config-if)#
```

40-19 lldp subtype

This command is used to configure the subtype of LLDP TLV(s).

lldp subtype port-id {mac-address | local}

Parameters

port-id	Specifies the subtype of the port ID TLV.
mac-address	Specifies the subtype of the port ID TLV to “MAC Address (3)” and the field of “port ID” will be encoded with the MAC address.
local	Specifies the subtype of the port ID TLV to use “Locally assigned (7)” and the field of “port ID” will be encoded with the port number.

Default

The subtype of port ID TLV is local (port number).

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to specify the subtype of LLDP TLV(s). A port ID subtype is used to indicate how the port is being referenced in the port ID field.

Example

This example shows how to configure the subtype of the port ID TLV to mac-address.

```
Switch# configure terminal
Switch(config)# interface ethe1/0/1
Switch(config-if)# lldp subtype port-id mac-address
Switch(config-if)#
```

40-20 show lldp

This command is used to display the general LLDP configuration of the Switch.

show lldp

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the global LLDP configuration of the Switch.

Example

This example shows how to display the global LLDP configuration of the Switch.

```
Switch#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : F0-7D-68-12-10-01
    System Name               : Switch
    System Description        : 10 Gigabit Ethernet Smart Managed Switch
    System Capabilities Supported: Repeater, Bridge
    System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         :
    Software Revision         : 1.00.021
    Serial Number             : DXS1210102030
    Manufacturer Name         : D-Link Corporation
    Model Name                : DXS-1210-28T
    Asset ID                  :

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

40-21 show lldp interface

This command is used to display the LLDP configuration at the physical interface.

show lldp interface *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to display the LLDP information of each physical interface.

Example

This example shows how to display the LLDP configuration on port 1.

```
Switch# show lldp interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID                                                 :eth1/0/1
Admin Status                                            :TX and RX
Notification                                            :Disabled
Basic Management TLVs:
    Port Description                                    :Disabled
    System Name                                         :Disabled
    System Description                                  :Disabled
    System Capabilities                                 :Disabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                        :Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                        :Disabled
    Power Via MDI                                       :Disabled
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                           :Disabled
    LLDP-MED Network Policy TLV                         :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV             :Disabled
    LLDP-MED Inventory TLV                              :Disabled

Switch#
```

Display Parameters

Enabled Management Address	Displays the enabled IPv4/IPv6 addresses. The indicated string “(None)” means that the user did not configure the management address with the lldp management-address command or the enabled default IPv4 and IPv6 addresses are not applicable.
Enabled Port and Protocol VLAN ID	This indicating string is shown when there are enabled port and protocol VLANs. The VLAN list is the configured enabled VLANs. If there is no configured PPVID VLAN, the string is “(None)”.
Enabled VLAN Name	This indicating string is shown when there are enabled VLANs for sending VLAN Name TLVs. The VLAN list includes the configured enabled VLANs. If there is no configured VLAN for the VLAN Name TLV, the string is “(None)”.

Enabled Protocol Identity	Displays the enabled protocol string for protocol identity TLVs. If there is no enabled protocol for protocol identity TLVs, the string is “(None)”.

40-22 show lldp local interface

This command is used to display physical interface information that will be carried in the LLDP TLVs and sent to neighbor devices.

show lldp local interface *INTERFACE-ID* **[, | -] [brief | detail]**

Parameters

INTERFACE-ID	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
brief	(Optional) Specifies to display the information in brief mode.
detail	(Optional) Specifies to display the information in detailed mode. If neither brief nor detail is specified, display the information in the normal mode.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to display each physical interface’s local LLDP information currently available for populating outbound LLDP advertisements.

Example

This example shows how to display the local information of port 1 in detailed mode.

```
Switch#show lldp local interface eth1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DXS-1210-28T HW
                                           A1 firmware 1.00.021 Port 1 on Unit
                                           1
Port PVID                                : 1
Management Address Count                 : 2

    Address 1 : (default)
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.139.6.1

    Address 2 :
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.139.6.1

PPVID Entries Count                      : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the local information of port 1 in normal mode.

```
Switch#show lldp local interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DXS-1210-28T HW
                                           A1 firmware 1.00.021 Port 1 on Unit
                                           1
Port PVID                                : 1
Management Address Count                 : 2
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536
LLDP-MED capabilities                    : (See Detail)
Network Policy                           : (See Detail)


Switch#
```

This example shows how to display local information of port 1 in brief mode.

```
Switch#show lldp local interface eth1/0/1 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DXS-1210-28T HW
                                           A1 firmware 1.00.021 Port 1 on Unit
                                           1


Switch#
```

40-23 show lldp management-address

This command is used to display the management address information.

show lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Parameters

IP-ADDRESS	(Optional) Specifies to display the LLDP management information for a specific IPv4 address.
IPV6-ADDRESS	(Optional) Specifies to display the LLDP management information for a specific IPv6 address.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the management address information.

Example

This example shows how to display all management address information.

```
Switch#show lldp management-address

Address 1 : (default)
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.165.2.1
    Advertising Ports                : -

Address 2 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.165.2.1
    Advertising Ports                : -

Total Entries : 2


Switch#
```

40-24 show lldp neighbor interface

This command is used to display each physical interface's information currently learned from the neighbor.

show lldp neighbors interface INTERFACE-ID [, | -] [brief | detail]

Parameters

INTERFACE-ID	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
brief	(Optional) Specifies to display the information in brief mode.
detail	(Optional) Specifies to display the information in detailed mode. If neither brief nor detail is specified, display the information in the normal mode.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the information learned from the neighbor devices.

Example

This example shows how to display detailed LLDP information about neighboring devices connected to port 9.

```
Switch# show lldp neighbors interface eth1/0/9 detail

Port ID: eth1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : F0-7D-68-30-36-00
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/10
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
        (None)

    Port PVID                               : 0
    PPVID Entries Count                     : 0
        (None)

    VLAN Name Entries Count                 : 0
        (None)

    Protocol ID Entries Count               : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display normal LLDP information about neighboring devices connected to port 9.

```
Switch# show lldp neighbors interface eth1/0/9

Port ID: eth1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : F0-7D-68-30-36-00
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/10
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
    Port PVID                               : 0
    PPVID Entries Count                     : 0
    VLAN Name Entries Count                 : 0
    Protocol ID Entries Count               : 0
    MAC/PHY Configuration/Status            : (None)
    Power Via MDI                           : (None)
    Link Aggregation                        : (None)
    Maximum Frame Size                      : 0
    LLDP-MED capabilities                   : (See Detail)
    Extended power via MDI                  : (See Detail)
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display brief LLDP information about neighboring devices connected to port 9.

```
Switch# show lldp neighbors interface eth1/0/9 brief

Port ID: eth1/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : F0-7D-68-30-36-00
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/10
    Port Description                        :


Switch#
```

40-25 show lldp traffic

This command is used to display the global LLDP traffic information of the Switch.

show lldp traffic

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display an overview of neighbor detection activities on the Switch.

Example

This example shows how to display global LLDP traffic information.

```
Switch# show lldp traffic

Last Change Time  : 0D2H6M40S
Total Inserts     : 1
Total Deletes     : 0
Total Drops       : 0
Total Ageouts     : 0

Switch#
```

Display Parameters

Last Change Time	The amount of time since the last update to the remote table in days, hours, minutes, and seconds.
Total Inserts	Total number of inserts to the remote data table.
Total Deletes	Total number of deletes from the remote data table.
Total Drops	Total number of times the complete remote data received was not inserted due to insufficient resources.
Total Ageouts	Total number of times a complete remote data entry was deleted because the Time to Live interval expired.

40-26 show lldp traffic interface

This command is used to display the each physical interface's LLDP traffic information.

show lldp traffic interface *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display LLDP traffic on each physical interface.

Example

This example shows how to display statistics information of port 1.

```
Switch# show lldp traffic interface eth1/0/1

Port ID : eth1/0/1
-------------------------------------------
    Total Transmits     : 0
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 0
    Total TLV Discards  : 0
    Total TLV Unknowns  : 0
    Total Ageouts       : 0

Switch#
```

Display Parameters

Total Transmits	The total number of LLDP packets transmitted on the port.
Total Discards	The total number of LLDP frames discarded on the port for any reason.
Total Errors	The number of invalid LLDP frames received on the port.
Total Receives	The total number of LLDP packets received on the port.
Total TLV Discards	The number of TLVs discarded.
Total TLV Unknowns	The total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
Total Ageouts	The total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.

41. Loopback Detection (LBD) Commands

41-1 loopback-detection (Global)

This command is used to enable the loopback detection function globally. Use the **no** form of this command to disable the function globally.

loopback-detection [mode {port-based | vlan-based}]

no loopback-detection [mode]

Parameters

mode	(Optional) Specifies the detection mode.
port-based	(Optional) Specifies that the loop detection will work in the port-based mode.
vlan-based	(Optional) Specifies that the loop detection will work in the VLAN-based mode.

Default

By default, this option is disabled.

By default, the detection mode is port-based.

Command Mode

Global Configuration Mode.

Usage Guideline

Generally, port-based loop detection is used in ports that are connected to users, and VLAN-based detection is used in trunk ports when the partner switch does not support the loop detection function.

When doing port-based detection, the LBD enabled port will send untagged port-based LBD packets out from the port to discover the loop. If there is a loop occurrence on the path, then the packet being transmitted will loop back to the same port or to another port located on the same device. When an LBD enabled port detects a loop condition, packet transmitting and receiving is disabled at the port.

When doing VLAN-based detection, the port will periodically send VLAN-based LBD packets for each VLAN that the port has membership of the VLAN is enabled for loop detection. If the port is a tagged member of the detecting VLAN, tagged LBD packets are sent. If the port is an untagged member of the detecting VLAN, untagged LBD packets are sent. If there is a loop occurrence on the VLAN path, then packet transmitting and receiving will be temporarily stopped on the looping VLAN at the port where the loop is detected.

If an LBD disabled port receives an LBD packet and detects that the packet is sent out by the system itself, the sending port will be blocked if the packet is a port-based LBD packet, or the VLAN of the sending port will be blocked if the packet is a VLAN-based LBD packet.

If the port is configured for VLAN-based and if the port is an untagged member of multiple VLANs, then the port will send one untagged LBD packet for each VLAN with the VLAN number specified in the VLAN field of the packet.

There are two ways to recover an error disabled port. The user can use the **errdisable recovery cause loopback-detect** command to enable the auto-recovery of ports that were disabled by loopback detection. Alternatively, manually recover the port by entering the **shutdown** command followed by the **no shutdown** command for the port.

The VLAN being blocked on a port can be automatically recovered, if the **errdisable recovery cause loopback-detect** command is configured. Alternatively, manually recover the operation by entering the **shutdown** command followed by the **no shutdown** command for the port.

Example

This example shows how to enable the port-based loopback detection function globally and set the detection mode to port-based.

```
Switch# configure terminal
Switch(config)# loopback-detection
Switch(config)# loopback-detection mode port-based
Switch(config)#
```

41-2 loopback-detection (Interface)

This command is used to enable the loopback detection function for an interface. Use the **no** form of this command to disable the function for an interface.

loopback-detection

no loopback-detection

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

Use this command to enable or disable the loopback detection function on an interface.

Example

This example shows how to enable the loopback detection function on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# loopback-detection
Switch(config-if)#
```

41-3 loopback-detection interval

This command is used to configure the timer interval. Use the **no** form of this command to revert to the default setting.

loopback-detection interval *SECONDS*

no loopback-detection interval

Parameters

SECONDS	Specifies the interval in seconds at which LBD packets are transmitted. The valid range is from 1 to 32767.

Default

By default, this value is 10 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the interval at which LBD packets are sent to discover the loop occurrence.

Example

This example shows how to configure the time interval to 20 seconds.

```
Switch# configure terminal
Switch(config)# loopback-detection interval 20
Switch(config)#
```

41-4 loopback-detection vlan

This command is used to configure the VLANs to be enabled for loopback detection. Use the **no** form of this command to revert to the default setting.

loopback-detection vlan *VLAN-LIST*

no loopback-detection vlan *VLAN-LIST*

Parameters

VLAN-LIST	Specifies the VLAN identification number, numbers, or range of numbers to be matched. Enter one or more VLAN values separated by commas or hyphens for a range list.

Default

By default, this option is enabled for all VLANs.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the list of VLANs that are enabled for loop detection. The command setting takes effect when the port's loop detection mode is operated in the VLAN-based mode.

By default, LBD Control packets are sent out for all VLANs that the port is a member of. LBD Control packets will be sent out for the VLAN that the member port within the specified VLAN list.

The VLAN list can be incremented by issuing this command multiple times.

Example

This example shows how to enable VLANs 100 to 200 for loop detection.

```
Switch# configure terminal
Switch(config)# loopback-detection vlan 100-200
Switch(config)#
```

41-5 show loopback-detection

This command is used to display the current loopback detection control settings..

show loopback-detection [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the loopback detection setting and status.

Example

This example shows how to display the current loopback detection settings and status.

```
Switch#show loopback-detection

 Loop Detection       : Disabled
 Detection Mode       : port-based
 LBD enabled VLAN     : all VLANs
 Interval             : 10 seconds
 Action Mode          : Shutdown
 Address Type         : Multicast
 Function Version     : v4.07

 Interface         State       Result               Time Left (sec)
 --------------    --------    -----------------    ---------------
 eth1/0/1          Disabled    Normal               -
 eth1/0/2          Disabled    Normal               -
 eth1/0/3          Disabled    Normal               -
 eth1/0/4          Disabled    Normal               -
 eth1/0/5          Disabled    Normal               -
 eth1/0/6          Disabled    Normal               -
 eth1/0/7          Disabled    Normal               -
 eth1/0/8          Disabled    Normal               -
 eth1/0/9          Disabled    Normal               -
 eth1/0/10         Disabled    Normal               -
 eth1/0/11         Disabled    Normal               -
 eth1/0/12         Disabled    Normal               -
 eth1/0/13         Disabled    Normal               -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the loopback detection status for port 1.

```
Switch# show loopback-detection interface eth1/0/1

Interface        State       Result               Time Left (sec)
-------------    --------    ------------------   ------------
eth1/0/1         Disabled    Normal               -

Switch#
```

Display Parameters

Interface	Indicates the port that has loopback detection enabled.
Status	Indicates the function state on the port.
Result	Indicates whether a loop is detected.
Time Left	The remaining time before being auto-recovered.

41-6 loopback-detection action

This command is used to configure the loopback-detection mode. Use the **no** form of this command to revert to the default setting.

loopback-detection action {shutdown | none}

no loopback-detection action

Parameters

shutdown	Specifies to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected.
none	Specifies not to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected.

Default

By default, this mode is **shutdown**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the loopback-detection mode mode.

Example

This example shows how to configure the loopback-detection mode mode.

```
Switch# configure terminal
Switch(config)# loopback-detection action none
Switch(config)#
```

41-7 snmp-server enable traps loopback-detection

This command is used to enable the sending of SNMP notifications for loopback detection. Use the **no** form of this command to revert to the default setting.

snmp-server enable traps loopback-detection

no snmp-server enable traps loopback-detection

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for loopback detection.

Example

This example shows how to enable the sending of SNMP notifications for loopback detection.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps loopback-detection.
Switch(config)#
```

41-8 loopback-detection address-type

This command is used to configure the DA type of loopback-detection packets. Use the **no** form of this command to revert to the default setting.

loopback-detection address-type {multicast | broadcast}

no loopback-detection address-type

Parameters

multicast	Specifies to only send multicast LBD packets. The DA is CF-00-00-00-00-00.
broadcast	Specifies to only send broadcast LBD packets. The DA is FF-FF-FF-FF-FF-FF.

Default

By default, this mode is **multicast**.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the DA type of loopback-detection packets.

Example

This example shows how to configure the DA type of loopback-detection packets to broadcast.

```
Switch#configure terminal
Switch(config)#loopback-detection address-type broadcast
Switch(config)#
```

42. Mirror Commands

42-1 monitor session destination interface

This command is used to configure the destination interface for a port monitor session, allowing packets on source ports to be monitored via a destination port. Use the **no** form of this command to delete a port monitor session or remove the destination interface of the session.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

no monitor session *SESSION-NUMBER*

Parameters

session *SESSION-NUMBER*	Specifies the session number for the port monitor session. The value is from 1 to 4.
interface *INTERFACE-ID*	Specifies the destination interface for the port monitor session.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the destination interface for a local monitor session.

Both physical ports and port channels are valid as destination interfaces for monitor sessions. For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously. An interface can be configured as the destination interface of multiple sessions, but it can be a source interface of only one session.

Example

This example shows how to create a port monitor session with the session number 1. It assigns the physical port 1 as the destination port and three physical source ports 2 to 4 as monitor source ports.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth1/0/1
Switch(config)# monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

42-2 monitor session source interface

This command is used to configure the source port of a port monitor session. Use the **no** form of this command to remove a port monitor session or remove a source port from the port monitor session.

monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -] [both | rx | tx]**

no monitor session *SESSION-NUMBER* **source interface** *INTERFACE-ID* **[, | -]**

no monitor session *SESSION-NUMBER*

Parameters

session *SESSION-NUMBER*	Specifies the session number for the port monitor session. The value is from 1 to 4.
interface *INTERFACE-ID*	Specifies the source interface for a port monitor session.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
both	(Optional) Specifies to monitor the packets transmitted and received on the port.
rx	(Optional) Specifies to monitor the packets received on the port.
tx	(Optional) Specifies to monitor the packets transmitted on the port without forwarding, which means regardless of the port's STG status.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Both physical ports and port channels are valid as source interfaces of monitor sessions.

For a monitor session, multiple source interfaces can be specified, but only one destination interface can be specified. An interface cannot be a source interface of one session and destination port of another session simultaneously. An interface can be configured as destination interface of multiple sessions, but it can be a source interface of only one session.

If the direction is not specified, both TX (transmitted) and RX (received) traffic are monitored.

Example

This example shows how to create a port monitor session with session number 1. It assigns the physical port 1 as the destination port and three source physical ports 2 to 4 as monitor source ports.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface eth1/0/1
Switch(config)# monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

42-3 show monitor session

This command is used to display all or a specific port mirroring session.

show monitor session [*SESSION-NUMBER***]**

Parameters

SESSION-NUMBER	(Optional) Specifies the session number to be displayed. The value is from 1 to 4.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all monitor sessions will be displayed.

Example

This example shows how to display a created port monitor session with the session number 1.

```
Switch#show monitor session 1

 Session 1
     Session Type: local session
     Destination Port: eth1/0/1
     Source Ports:
         Both:
             eth1/0/2
             eth1/0/3
             eth1/0/4

 Total Entries: 1

Switch#
```

43. Multicast Listener Discovery (MLD) Snooping Commands

43-1 clear ipv6 mld snooping statistics

This command is used to clear the statistic counter of the Switch.

clear ipv6 mld snooping statistics {all | vlan *VLAN-ID* **| interface** *INTERFACE-ID***}**

Parameters

all	Specifies to clear IPv6 MLD snooping statistics for all VLANs and all ports.
vlan *VLAN-ID*	Specifies the VLAN to be used.
interface *INTERFACE-ID*	Specifies the interface to be used.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the statistic counter of the Switch.

Example

This example shows how to clear all MLD snooping statistics.

```
Switch# clear ipv6 mld snooping statistics all
Switch#
```

43-2 ipv6 mld snooping

This command is used to enable MLD snooping. Use the **no** form of this command to disable MLD snooping.

ipv6 mld snooping

no ipv6 mld snooping

Parameters

None.

Default

MLD snooping is disabled on all VLANs.

The MLD snooping global state is disabled by default.

Command Mode

VLAN Configuration Mode.

Global Configuration Mode.

Usage Guideline

For a VLAN to operate with MLD snooping, both the global state and per VLAN state must be enabled. On a VLAN, the setting of IGMP snooping and MLD snooping are independent. That is, IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

Example

This example shows how to disable MLD snooping globally.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

This example shows how to enable MLD snooping globally.

```
Switch# configure terminal
Switch(config)# ipv6 mld snooping
Switch(config)#
```

This example shows how to enable MLD snooping on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping
Switch(config-vlan)#
```

43-3 ipv6 mld snooping fast-leave

This command is used to configure MLD snooping fast-leave in the VLAN. Use the **no** form of this command to disable the fast-leave option in the specified VLAN.

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to allow MLD membership to be immediately removed from a port when receiving the leave message without using the group specific or group-source specific query mechanism.

Example

This example shows how to enable MLD snooping fast-leave on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping fast-leave
Switch(config-vlan)#
```

43-4 ipv6 mld snooping last-listener-query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping last-listener-query-interval *SECONDS*

no ipv6 mld snooping last-listener-query-interval

Parameters

SECONDS	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

VLAN Configuration Mode.

Usage Guideline

On receiving an MLD done message, the MLD snooping querier will assume that there are no local members in the VLAN if there are no reports received after the response time. Users can lower this interval to reduce the amount of time it takes a switch to detect the loss of the last member of a group.

Example

This example shows how to configure the last-listener query interval time to be 3 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

43-5 ipv6 mld snooping mrouter

This command is used to configure the specified interface(s) as the router ports or forbidden to be IPv6 multicast router ports in the VLAN on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden IPv6 multicast router ports.

ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -] | learn pimv6}**

no ipv6 mld snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -] | learn pimv6}**

Parameters

interface	Specifies a range of interfaces as being connected to multicast-enabled routers.
forbidden interface	Specifies a range of interfaces as being not connected to multicast-enabled routers.
INTERFACE-ID	Specifies the interfaces to be displayed. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
learn pimv6	Specifies to enable dynamic learning of multicast router port.

Default

No IPv6 MLD snooping multicast router port is configured.

Auto-learning is enabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be member port of the configured VLAN.

The multicast router port can be either dynamically learned or statically configured into an MLD snooping entity. With the dynamic learning, the MLD snooping entity will listen to MLD and PIMv6 packet to identify whether the partner device is a router.

Example

This example shows how to configure port 1 as an MLD snooping multicast router port and port 2 as an MLD snooping forbidden multicast router port on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping mrouter interface eth1/0/1
Switch(config-vlan)# ipv6 mld snooping mrouter forbidden interface eth1/0/2
Switch(config-vlan)#
```

This example shows how to disable the auto-learning of routing protocol packets on VLAN 4.

```
Switch# configure terminal
Switch(config)# vlan 4
Switch(config-vlan)# no ipv6 mld snooping mrouter learn pimv6
Switch(config-vlan)#
```

43-6 ipv6 mld snooping querier

This command is used to enable the MLD snooping querier on the Switch. Use the **no** form of this command to disable the MLD snooping querier function.

ipv6 mld snooping querier

no ipv6 mld snooping querier

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

If the system can play the querier role, the entity will listen for MLD query packets sent by other devices. If MLD query message is received, the device with lower value of IPv6 address becomes the querier.

Example

This example shows how to enable the MLD snooping querier state on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping querier
Switch(config-vlan)#
```

43-7 ipv6 mld snooping query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD general query messages periodically. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping query-interval *SECONDS*

no ipv6 mld snooping query-interval

Parameters

SECONDS	Specifies to configure the interval at which the designated router sends MLD general-query messages. The range is 1 to 31744.

Default

By default, this value is 125 seconds.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The query interval is the interval between General Queries sent by the Querier. By varying the query interval, an administrator may tune the number of MLD messages on the network; larger values cause MLD Queries to be sent less often.

Example

This example shows how to configure the MLD snooping query interval to 300 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

43-8 ipv6 mld snooping query-max-response-time

This command is used to configure the maximum response time advertised in MLD snooping queries. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping query-max-response-time SECONDS

no ipv6 mld snooping query-max-response-time

Parameters

SECONDS	Specifies to set the maximum response time in seconds advertised in MLD Snooping queries. The range is from 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to configure the period of which the group member can respond to an MLD query message before the MLD Snooping deletes the membership.

Example

This example shows how to configure the maximum response time to 20 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

43-9 ipv6 mld snooping query-version

This command is used to configure the general query packet version sent by the MLD snooping querier. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping query-version *NUMBER*

no ipv6 mld snooping query-version

Parameters

NUMBER	Specifies that the version of the MLD general query sent by MLD snooping querier. The value is 1 and 2.

Default

By default, this version number is 2.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to configure the general query packet version sent by the MLD snooping querier.

Example

This example shows how to configure the query version to be 1 on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-version 1
Switch(config-vlan)#
```

43-10 ipv6 mld snooping report-suppression

This command is used to enable MLD report suppression on a VLAN. Use the **no** form of this command to disable report suppression on a VLAN.

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The report suppression function only works for MLDv1 traffic.

When report suppression is enabled, the Switch suppresses duplicate reports sent by hosts. Suppression for the same group report or leave messages will continue until the suppression time expires. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.

Example

This example shows how to enable MLD report suppression.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# ipv6 mld snooping report-suppression
Switch(config-vlan)#
```

43-11 ipv6 mld snooping robustness-variable

This command is used to set the robustness variable used in MLD snooping. Use the **no** form of this command to revert to the default value.

ipv6 mld snooping robustness-variable *VALUE*

no ipv6 mld snooping robustness-variable

Parameters

VALUE	Specifies the robustness variable. The range is from 1 to 7.

Default

By default, this value is 2.

Command Mode

VLAN Configuration Mode.

Usage Guideline

The robustness variable provides fine-tuning to allow for expected packet loss on an interface. The value of the robustness variable is used in calculating the following MLD message intervals:

- **Group member interval** - Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval).
- **Other querier present interval** - Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval).
- **Last listener query count** - The number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable.

User can increase this value if a subnet is expected to be loose.

Example

This example shows how to configure the robustness variable to be 3 on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

43-12 ipv6 mld snooping static-group

This command is used to configure an MLD snooping static group. Use the **no** form of this command to delete a static group.

ipv6 mld snooping static-group *IPV6-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ipv6 mld snooping static-group *IPV6-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

IPV6-ADDRESS	Specifies an IPv6 multicast group address.
interface *INTERFACE-ID*	Specifies the interfaces to be configured. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, no static-group is configured.

Command Mode

VLAN Configuration Mode.

Usage Guideline

This command applies to MLD snooping in a VLAN to statically add group membership entries.

Use this command to create an MLD snooping static group in case that the attached host does not support MLD protocol.

Example

This example shows how to statically add group records for MLD snooping on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface eth1/0/5
Switch(config-vlan)#
```

43-13 ipv6 mld snooping suppression-time

This command is used to configure the time for suppressing duplicate MLD reports or leaves. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping suppression-time *SECONDS*

no ipv6 mld snooping suppression-time

Parameters

SECONDS	Specifies to configure the time for suppressing duplicates MLD reports. The range is 1 to 300.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Report suppression will suppress the duplicate MLD report or leave packets received in the suppression time. A small suppression time will cause the duplicate MLD packets be sent more frequently.

Example

This example shows how to configure the suppression time to be 125 on VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

43-14 ipv6 mld snooping minimum-version

This command is used to configure the minimum version of MLD hosts which MLD that is allowed in the VLAN. Use the **no** form of this command to remove the restriction from the VLAN.

ipv6 mld snooping minimum-version 2

no ipv6 mld snooping minimum-version

Parameters

None.

Default

No limit on minimum version.

Command Mode

VLAN Configuration Mode.

Usage Guideline

This setting only applies to filtering of MLD membership reports.

Example

This example shows how to restrict all MLDv1 hosts to join VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

43-15 show ipv6 mld snooping

This command is used to display MLD snooping information on the Switch.

show ipv6 mld snooping [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, MLD snooping information for all VLANs on which MLD snooping are enabled will be displayed.

Example

This example shows how to display MLD snooping information.

```
Switch#show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
    MLD snooping state           : Enabled
    Minimum version              : v1
    Fast leave                   : Disabled (port-based)
    Report suppression           : Disabled
    Suppression time             : 10 seconds
    Mrouter port learning        : Enabled
    Querier state                : Disabled
    Query version                : v2
    Query interval               : 125 seconds
    Max response time            : 10 seconds
    Robustness value             : 2
    Last listener query interval : 1 seconds

Total Entries: 1

Switch#
```

43-16 show ipv6 mld snooping groups

This command is used to display MLD snooping dynamic group information learned on the Switch.

show ipv6 mld snooping groups [*IPV6-ADDRESS* **| vlan** *VLAN-ID***] [detail]**

Parameters

IPV6-ADDRESS	(Optional) Specifies the group IP address. If no IPv6 address is specified, all MLD group information will be displayed.

vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD group information about all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
detail	(Optional) Specifies to display the MLD group detail information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display MLD snooping dynamic group information.

Example

This example shows how to display MLD snooping dynamic group information.

```
Switch# show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3

Switch#
```

This example shows how to display MLD snooping group detail information.

```
Switch# show ipv6 mld snooping groups detail

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3
  1/0/3
    version: v2, filter mode: Include, uptime: 0DT00H00M09S, expires: 0DT00H00M00S
      source 2000::1, uptime: 0DT00H00M09S, expires: 0DT00H04M11S

Switch#
```

43-17 show ipv6 mld snooping mrouter

This command is used to display MLD snooping multicast router information that has been automatically learned and manually configured on the Switch.

show ipv6 mld snooping mrouter [vlan *VLAN-ID* **[, | -]]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD snooping Multicast Router Information on all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

Example

This example shows how to display MLD snooping multicast router information.

```
Switch#show ipv6 mld snooping mrouter

VLAN   Ports
-----  -----------------------------
1      eth1/0/4 (static)
       eth1/0/2 (forbidden)

Total Entries: 1

Switch#
```

43-18 show ipv6 mld snooping static-group

This command is used to display MLD snooping static group information on the Switch.

show ipv6 mld snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IPv6 address to be displayed.
vlan *VLAN-ID*	Optional) Specifies the VLAN ID to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the MLD snooping static group information.

Example

This example shows how to display MLD snooping static group information.

```
Switch#show ipv6 mld snooping static-group

VLAN ID Group address                          Interface
------- ------------------------------------- ------------------
1       FF1E::1                                eth1/0/6

Total Entries: 1

Switch#
```

43-19 show ipv6 mld snooping statistics

This command is used to display MLD snooping statistics information on the Switch.

show ipv6 mld snooping statistics {interface [*INTERFACE-ID***[, | -]] | vlan [***VLAN-ID* **[, | -]]}**

Parameters

interface	Specifies to display statistics counters by interface.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan	Specifies to display statistics counters by VLAN.
VLAN-ID	(Optional) Specifies the VLAN ID to be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the MLD snooping related statistics information.

Example

This example shows how to display MLD snooping statistics information on port 4.

```
Switch# show ipv6 mld snooping statistics interface eth1/0/4

Interface eth1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Total Entries: 1

Switch#
```

This example shows how to display MLD snooping statistics information of VLAN 1.

```
Switch# show ipv6 mld snooping statistics vlan 1
VLAN 1 Statistics:
  Rx: V1Report 3, v2Report 0, Query 3, v1Done 0
  Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 1
Switch#
```

44. Multiple Spanning Tree Protocol (MSTP) Commands

44-1 instance

This command is used to map VLANs to an MST instance. Use the **no instance** *INSTANCE-ID* command to remove the specified MST instance. Use the **no instance** *INSTANCE-ID* **vlans** *VLAND-ID* **[, | -]** command to return the VLANs to the default instance (CIST).

instance *INSTANCE-ID* **vlans** *VLAND-ID* **[, | -]**

no instance *INSTANCE-ID* **[vlans** *VLAND-ID* **[, | -]]**

Parameters

INSTANCE-ID	Specifies the MSTP instance identifier to which the specified VLANs are mapped. This value must be between 1 and 32.
vlans *VLAN-ID*	Specifies the VLANs to be mapped to or removed from the specified instance. This value must be between 1 and 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

MST Configuration Mode.

Usage Guideline

Any unmapped VLAN is mapped to the CIST instance. When mapping the VLANs to an instance, if the instance does not exist, this instance will be created automatically. If all VLANs of an instance are removed, this instance will be destroyed automatically. In another way, users can remove the instance manually by using the **no instance** command without VLANs specified.

Example

This example shows how to map a range of VLANs to instance 2.

```
Switch#configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 2 vlans 1-100
Switch(config-mst)#
```

44-2 name

This command is used to configure the name of an MST region. Use the **no** form of this command to revert to the default setting.

name *NAME*

no name *NAME*

Parameters

NAME	Specifies the name given for a specified MST region. The name string has a maximum length of 32 characters and the type is a general string which allows spaces.

Default

The default name is the MAC address of the Switch.

Command Mode

MST Configuration Mode.

Usage Guideline

Two or more switches with the same VLAN mapping and configuration version number are considered to be in different MST regions if the region names are different.

Example

This example shows how to configure the MSTP configuration name to “MName”.

```
Switch#configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# name MName
Switch(config-mst)#
```

44-3 revision

This command is used to configure the revision number for the MST configuration. Use the **no** form of this command to revert to the default setting.

revision *VERSION*

no revision

Parameters

VERSION	Specifies the revision number for the MST configuration. The range is from 0 to 65535.

Default

By default, this value is 0.

Command Mode

MST Configuration Mode.

Usage Guideline

Two Ethernet switches that have the same configuration but different revision numbers are considered to be part of two different regions.

Example

This example shows how to configure the revision level of the MSTP configuration to 2.

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# revision 2
Switch(config-mst)#
```

44-4 show spanning-tree mst

This command is used to display the information that used in the MSTP version.

show spanning-tree mst [configuration [digest]]

show spanning-tree mst [instance *INSTANCE-ID* **[, | -]] [interface** *INTERFACE-ID* **[, | -]] [detail]**

Parameters

configuration	(Optional) Specifies the MST configuration of the equipment.
digest	(Optional) Specifies to display the MD5 digest included in the current MST configuration identifier (MSTCI).
instance *INTANCE-ID*	(Optional) Specifies the instance number to be displayed.
,	(Optional) Specifies a series of instances or separates a range of instances from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of instances. No space is allowed before or after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the MSTP configuration and operation status. If a private VLAN is configured and the secondary VLAN does not map to the same primary VLAN, the show spanning-tree mst configuration command will display a message to indicate this condition.

Example

This example shows how to display MSTP detailed information.

```
Switch#show spanning-tree mst detail

 Spanning tree: Disabled,protocol: RSTP
 Number of MST instances: 1

 >>>>MST00  vlans mapped : 1-4094
 Bridge address: F0-7D-68-12-10-01, priority: 32768 (32768 sysid 0)
 Designated root address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  external root cost : 0
 Regional root bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  internal root cost : 0
 Designated bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 Topology changes count: 0

 eth1/0/1
   Port state: forwarding
   Port role: nonStp
   Port info : port id 128.1, priority: 128, cost: 200000
   Designated root address: 00-00-00-00-00-00, priority: 0
   Regional root address: 00-00-00-00-00-00, priority: 0
   Designated bridge address: 00-00-00-00-00-00, priority: 0, port id: 0.0

 eth1/0/3
   Port state: forwarding
   Port role: nonStp
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display MSTP detailed information of port 1.

```
Switch# show spanning-tree mst interface eth1/0/1 detail

eth1/0/1
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: non-edge
 Bpdu statistic counter: sent: 0, received: 0

 >>>>MST instance: 00,  vlans mapped : 1-4094
 Port state: forwarding
 Port role: nonStp
 Port info : port ID 128.1, priority: 128, cost: 200000
 Designated root address: 00-00-00-00-00-00, priority: 0
 Regional Root address: 00-00-00-00-00-00, priority: 0
 Designated bridge address: 00-00-00-00-00-00, priority: 0, port id: 0.0


Switch#
```

This example shows how to display MSTP summary information.

```
S Switch#show spanning-tree mst

 Spanning tree: Disabled,protocol: RSTP
 Number of MST instances: 1

 >>>>MST00  vlans mapped : 1-4094
 Bridge address: F0-7D-68-12-10-01, priority: 32768 (32768 sysid 0)
 Designated root address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  external root cost : 0
 Regional root bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 CIST  internal root cost : 0
 Designated bridge address: 00-00-00-00-00-00, priority: 0 (0 sysid 0)
 Topology changes count: 0

                                            Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/1       nonStp     forwarding 200000    128.1    p2p    non-edge
 eth1/0/3       nonStp     forwarding 200000    128.3    p2p    non-edge


Switch#
```

This example shows how to display MSTP summary information of ports 3 to 4.

```
Switch# show spanning-tree mst interface eth1/0/3-4

eth1/0/3
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: edge
 Bpdu statistic counter: sent: 4, received: 0

                                        Priority
 Instance Role       State      Cost      .Port#
 -------- ----       -----      ------    ---------
 MST00    designated forwarding 20000     128.3
 MST01    backup     blocking   200000    128.3

eth1/0/4
 Configured link type: auto, operation status: point-to-point
 Configured fast-forwarding: auto, operation status: edge
 Bpdu statistic counter: sent: 4, received: 0

                                        Priority
 Instance Role       State      Cost      .Port#
 -------- ----       -----      ------    ---------
 MST00    root       forwarding 20000     128.4
 MST01    backup     blocking   200000    128.4

Switch#
```

This example shows how to display MSTP summary information of ports 3 to 4 with instance 2.

```
Switch# show spanning-tree mst instance 2 interface eth1/0/3-4

 >>>>MST02 vlans mapped : 2-3
 Bridge Address: 00-12-d9-87-47-00 , Priority: 32770 (32768 sysid 2)
 Designated Root Address: 00-12-d9-87-47-00 , Priority: 32770
 Designated Bridge Address: 00-12-d9-87-47-00 , Priority: 32770
 Topology Changes Count: 0

                                            Priority Link
 Interface      Role       State      Cost      .Port#   Type   Edge
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/3       backup     blocking   200000    128.3    p2p    non-edge
 eth1/0/4       backup     blocking   200000    128.4    p2p    non-edge

Switch#
```

This example shows how to display MSTP instance mapping configuration.

```
Switch# show spanning-tree mst configuration

 Name     : MName
 Revision : 2,Instances configured: 3
 Instance    Vlans
 -------     ------------------------------------------------------------
       0     21-4094
       1     1-10
       2     11-20

Switch#
```

44-5 spanning-tree mst

This command is used to configure the path cost and port priority parameters for any MST instance (including the CIST with instance ID 0). Use the **no** form of this command to revert to the default setting.

spanning-tree mst *INSTANCE-ID* **{cost** *COST* **| port-priority** *PRIORITY***}**

no spanning-tree mst *INSTANCE-ID* **{cost | port-priority}**

Parameters

INSTANCE-ID	Specifies the MSTP instance identifier.
cost *COST*	Specifies the path cost for an instance. This value must be between 1 and 200000000.
port-priority *PRIORITY*	Specifies the port priority for an instance. This value must be between 0 and 240 in increments of 16.

Default

The cost is defined based on the port speed. The faster the speed is, the smaller cost value it is. MST always uses long path cost.

The port priority is 128.

Command Mode

Interface Configuration Mode.

Usage Guideline

When entering the cost value, do not include a comma in the entry. For example, enter 1000 instead of 1,000.

Example

This example shows how to configure the path cost of port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

44-6 spanning-tree mst configuration

This command is used to enter the MST Configuration Mode. Use the **no** form of this command to revert to the default setting.

spanning-tree mst configuration

no spanning-tree mst configuration

Parameters

None.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the MST Configuration Mode.

Example

This example shows how to enter the MST Configuration Mode.

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)#
```

44-7 spanning-tree mst max-hops

This command is used to configure the MSTP maximum hop count value. Use the **no** form of this command to revert to the default setting.

spanning-tree mst max-hops *HOP-COUNT*

no spanning-tree mst max-hops

Parameters

max-hops *HOP-COUNT*	Specifies the MSTP maximum hop count number. The range is from 1 to 40 hops.

Default

By default, this value is 20 hops.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the maximum hops for MSTP.

Example

This example shows how to configure the MSTP maximum hop count value.

```
Switch# configure terminal
Switch(config)# spanning-tree mst max-hops 19
Switch(config)#
```

44-8 spanning-tree mst hello-time

This command is used to configure the per-port hello time used in the MSTP version. Use the **no** form of this command to revert to the default setting.

spanning-tree mst hello-time *SECONDS*

no spanning-tree mst hello-time

Parameters

SECONDS	Specifies to determine the time interval to send one BPDU at the designated port. This value is either 1 or 2.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Usage Guideline

This MSTP hello-time only takes effect in the MSTP mode.

Example

This example shows how to configure the hello time used in MSTP version on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree mst hello-time 1
Switch(config-if)#
```

44-9 spanning-tree mst priority

This command is used to configure the bridge priority value for the selected MSTP instance. Use the **no** form of this command to revert to the default setting.

spanning-tree mst *INSTANCE-ID* **priority** *PRIORITY*

no spanning-tree mst *INSTANCE-ID* **priority**

Parameters

INSTANCE-ID	Specifies the MSTP instance identifier. Instance 0 represents the default instance, CIST.
PRIORITY	Specifies the bridge priority value that must be divisible by 4096. The range is from 0 to 61440.

Default

By default, this value is 32768.

Command Mode

Global Configuration Mode.

Usage Guideline

The priority has same meaning with as the bridge priority in the STP command reference, but can specify a different priority for distinct MSTP instances.

Example

This example shows how to configure the bridge priority for the MSTP instance 2.

```
Switch# configure terminal
Switch(config)# spanning-tree mst 2 priority 0
Switch(config)#
```

45. Neighbor Discovery (ND) Inspection Commands

45-1 ipv6 nd inspection policy

This command is used to create an ND inspection policy. This command will enter the ND Inspection Policy Configuration Mode. Use the **no** form of this command to remove the ND inspection policy.

ipv6 nd inspection policy *POLICY-NAME*

no ipv6 nd inspection policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the ND inspection policy name.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create an ND inspection policy. This command will enter the ND Inspection Policy Configuration Mode. ND inspection is mainly for inspection of Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

Example

This example shows how to create an ND policy name called “policy1”.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

45-2 validate source-mac

This command is used to check the source MAC address against the link-layer address for ND messages. Use the **no** form of this command to disable the check.

validate source-mac

no validate source-mac

Parameters

None.

Default

By default, this option is disabled.

Command Mode

ND Inspection Policy Configuration Mode.

Usage Guideline

When the Switch receives an ND message that contains a link-layer address, the source MAC address is checked against the link-layer address. The packet will be dropped if the link-layer address and the MAC addresses are different from each other.

Example

This example shows how to enable the Switch to drop an ND message whose link-layer address does not match the MAC address.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)#
```

45-3 device-role

This command is used to specify the role of the attached device. Use the **no** form of this command to revert to the default setting.

device-role {host | router}

no device-role

Parameters

host	Specifies to set the role of the device to host.
router	Specifies to set the role of the device to router.

Default

By default, the device's role is **host**.

Command Mode

ND Inspection Policy Configuration Mode.

Usage Guideline

Use this command to specify the role of the attached device. By default, the device's role is set as host and inspection for NS and NA messages are performed. If the device role is set as router, the NS and NA inspection is not performed. When performing NS/NA inspection, the message will be verified against the dynamic binding table learned from the ND protocol or from the DHCP.

Example

This example shows how to create a ND policy named "policy1" and configures the device's role to host.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)#
```

45-4 ipv6 nd inspection attach-policy

This command is used to apply an ND inspection policy on the specified interface. Use the **no** form of this command to remove the ND inspection policy.

ipv6 nd inspection attach-policy [*POLICY-NAME***]**

no ipv6 nd inspection attach-policy

Parameters

POLICY-NAME	(Optional) Specifies the ND inspection policy name.

Default

By default, ND inspection policy is not applied.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to apply the ND Inspection policy on a specified interface. If no parameter is specified, the behavior of the default policy is as follows:

- NS/NA messages are inspected.
- Layer 2 header source MAC address validations are disabled.

Example

This example shows how to apply ND inspection policy called “policy1” on port 3.

```
Switch# configure terminal
Switch(config)# ipv6 nd inspection policy policy1
Switch(config-nd-inspection)# device-role host
Switch(config-nd-inspection)# validate source-mac
Switch(config-nd-inspection)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

45-5 show ipv6 nd inspection policy

This command is used to display Router Advertisement (RA) guard policy information.

show ipv6 nd inspection policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the IPv6 RA guard policy name.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display Router Advertisement (RA) guard policy information. If no parameter is specified, information of all policies will be displayed.

Example

This example shows how to display the policy configuration for a policy named “inspect1”.

```
Switch# show ipv6 nd inspection policy inspect1

Policy inspect1 configuration:
   Device Role: host
   Validate Source MAC: Enabled
   Target: eth1/0/1-1/0/2

Switch#
```

46. Network Access Authentication Commands

46-1 authentication guest-vlan

This command is used to configure the guest VLAN setting. Use the **no** form of this command to remove the guest VLAN.

authentication guest-vlan *VLAN-ID*

no authentication guest-vlan

Parameters

VLAN-ID	Specifies the authentication guest VLAN.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command cannot be configured if the specified VLAN does not exist as a static VLAN. The host cannot access the network until it passes the authentication. If the guest VLAN is configured, the host is allowed to access the guest VLAN without passing the authentication. During authentication, if the RADIUS server assigns a VLAN to the user, then the user will be authorized to this assigned VLAN. Guest VLAN and VLAN assignment does not take effect on trunk VLAN port and VLAN tunnel port.

Normally guest VLAN and VLAN assignment are functioning for hosts that connect to untagged ports. It may cause unexpected behavior if it is functioning on hosts that send tagged packets.

If the authentication host-mode is set to **multi-host**, the port will be added as a guest VLAN member port and the PVID of the port will change to guest VLAN. Traffic that comes from guest VLAN can be forward whatever whether authenticated. Traffic that comes from other VLANs will still be dropped until it pass authentication. When one host passes authentication, the port will leave the guest VLAN and be added to the assigned VLAN. The PVID of the port will be changed to the assigned VLAN.

If the authentication host-mode is set to **multi-auth**, the port will be added as a guest VLAN member port and the PVID of the port will be changed to a guest VLAN. Hosts that are allowed to access the guest VLAN are forbidden to access other VLANs until it pass authentication. When one host passes authentication, the port will stay in the guest VLAN, the PVID of the port will not be changed.

If guest VLAN is disabled, the port will exit the guest VLAN and return to the native VLAN. The PVID will change to the native VLAN.

Example

This example shows how to specify VLAN 5 as a guest VLAN.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication guest-vlan 5
Switch(config-if)#
```

46-2 authentication host-mode

This command is used to specify the authentication mode. Use the **no** form of this command to revert to the default setting.

authentication host-mode {multi-host | multi-auth}

no authentication host-mode

Parameters

multi-host	Specifies the port to operate in the multi-host mode. Only a single authentication is performed and all hosts connected to the port are allowed.
multi-auth	Specifies the port to operate in the multi-auth mode. Each host will be authenticated individually.

Default

By default, **multi-auth** is used.

Command Mode

Interface Configuration Mode.

Usage Guideline

If the port is operated in the **multi-host** mode, and one of the hosts is authenticated, all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period.

If the port is operated in the **multi-auth** mode, each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.

Example

This example shows how to specify the port 1 to operate in the multi-host mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication host-mode multi-host
Switch(config-if)#
```

46-3 authentication periodic

This command is used to enable periodic re-authentication for a port. Use the **no** form of this command to disable periodic re-authentication.

authentication periodic

no authentication periodic

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to enable or disable periodic re-authentication for a port.

Example

This example shows how to enable periodic re-authentication on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication periodic
Switch(config-if)#
```

46-4 authentication timer reauthentication

This command is used to configure the timer to re-authenticate a session. Use the **no** form of this command to revert to the default setting.

authentication timer reauthentication {*SECONDS***}**

no authentication timer reauthentication

Parameters

SECONDS	Specifies the timer to re-authenticate a session. The range is from 1 to 65535.

Default

By default, this value is 3600 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure the re-authentication timer.

Example

This example shows how to configure the re-authentication timer value to 200 for port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication timer reauthentication 200
Switch(config-if)#
```

46-5 authentication timer restart

This command is used to configure the timer to restart the authentication after the last failed authentication. Use the **no** form of this command to revert to the default setting.

authentication timer restart *SECONDS*

no authentication timer restart

Parameters

SECONDS	Specifies the authentication restart timer value. The range is from 1 to 65535.

Default

By default, this value is 60 seconds.

Command Mode

Interface Configuration Mode.

Usage Guideline

The Switch will be in the quiet state for a failed authentication session until the expiration of the timer.

Example

This example shows how to configure the restart timer to 20 for port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication timer restart 20
Switch(config-if)#
```

46-6 authentication username

This command is used to create a user in the local database for authentication. Use the **no** form of this command to remove a user in the local database.

authentication username *NAME* **password** *PASSWORD* **[vlan** *VLAN-ID***]**

no authentication username *NAME* **[vlan]**

Parameters

NAME	Specifies the username with a maximum of 32 characters.
password *PASSWORD*	Specifies the password in the clear text form for authentication with a maximum of 32 characters.
vlan *VLAN-ID*	Specifies the VLAN to be assigned.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the local database used for user authentication.

Example

This example shows how to create a local account with user1 as the username and pass1 as password.

```
Switch# configure terminal
Switch(config)# authentication username user1 password pass1
Switch(config)#
```

46-7 clear authentication sessions

This command is used to remove authentication sessions.

clear authentication sessions { dot1x | all | interface *INTERFACE-ID* **[dot1x] | mac-address** *MAC-ADDRESS***}**

Parameters

dot1x	Specifies to clear all dot1x sessions.
all	Specifies to clear all sessions.
interface *INTERFACE-ID*	Specifies a port to clear sessions.
mac-address *MAC-ADDRESS*	Specifies a specific user to clear session.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the authentication sessions.

Example

This example shows how to remove authentication sessions on port 1.

```
Switch# clear authentication sessions interface eth1/0/1
Switch#
```

46-8 authentication max users

This command is used to configure the maximum authenticated users for the entire system or for a port. Use the **no** form of this command to revert to the default settings.

authentication max users *NUMBER*

no authentication max users

Parameters

NUMBER	Specifies to set the maximum authenticated users' number. The range is from 1 to 1000.

Default

None.

Command Mode

Global Configuration Mode.

Interface Configuration Mode.

Usage Guideline

This command can be used in the Global Configuration Mode and Interface Configuration Mode.

If the command is configured in the Global Configuration Mode, the maximum user number limits the user number of the entire system.

If the command is configured in the Interface Configuration Mode, the maximum user number is set for the interface.

This command is limited to 802.1X users.

In addition, the command has the following limitation:

- If the new maximum is less than the current number of users, the command will be rejected and the error message will be prompted.

Example

This example shows how to set the maximum authenticated users for system.

```
Switch# configure terminal
Switch(config)# authentication max users 256
Switch(config)#
```

46-9 authorization disable

This command is used to disable the acceptance of the authorized configuration. Use the **no** form to enable the acceptance of the authorized configuration.

authorization disable

no authorization disable

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example, VLAN) assigned by the RADIUS server will be accepted if the authorization status is enabled.

Example

This example shows how to enable the authorization status.

```
Switch# configure terminal
Switch(config)# no authorization disable
Switch(config)#
```

46-10 show authentication sessions

This command is used to display authentication information.

show authentication sessions [dot1x | interface *INTERFACE-ID* **[, | -] [dot1x] | mac-address** *MAC-ADDRESS***]**

Parameters

dot1x	(Optional) Specifies to display all dot1x sessions.
interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
mac-address *MAC-ADDRESS*	(Optional) Specifies to display a specific user.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, the sessions associated with all ports will be displayed.

Example

This example shows how to display sessions on port 1.

```
Switch#show authentication sessions interface eth1/0/1

Interface: eth1/0/1
MAC Address: 00-10-94-00-00-01
Authentication VLAN: 1
Authentication State: Success
Authentication Username: v4
Aging Time: 3600 sec
Method   State
  802.1X  : Success, Selected
  802.1X Authenticator State: AUTHENTICATED
  802.1X Backend State: IDLE

Total Authenticating Hosts: 0
Total Authenticated Hosts: 1
Total Blocked Hosts: 0

Switch#
```

Display Parameters

Interface	The authentication host received interface.
MAC Address	The MAC address of authentication host.
Authentication VLAN	The original VLAN of the host start authentication.
Authentication State	The authentication status of host. • **Start** - Host received, but no any authentication start. • **Initialization**- Authentication resource ready, but no new authentication start. • **Authenticating** - Host is under authenticating. • **Failure** - Authentication failure. • **Success** - Host pass authentication.
Authentication Username	It indicates the user name of host.
Assigned VLAN	Effectively assigned VLAN ID that was authorized after the host passed authentication.
Aging Time/Block Time	• **Aging Time** - Specifies a time period during which an authenticated host will be kept in an authenticated state. When the aging time has timed-out, the host will be moved back to an unauthenticated state. • **Blocked Time** - If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually.
Method	The Authentication method, such as 802.1X.
State	The method authentication state. • **Authenticating** - Host is under authentication by this method. • **Success** - Host pass this method authentication. • **Selected** - This method's authentication result is taken and parsed by system for the host. • **Failure** - Host fail at this method authentication. • **No Information** - Authentication info is unavailable.
802.1X Authenticator State	Indicates the 802.1X authenticator PAE state: It can be one of the following values:

	• **INITIALIZE** - Indicates the authenticator is initializing the state machine and ready to authenticate the supplicant. • **DISCONNECTED** - Indicates that the state machine initialization has finished, but no supplicant connects to this port. • **CONNECTING** - Indicates that the Switch has detected a supplicant connecting to this port. The PAE will attempt to establish communication with a supplicant. • **AUTHENTICATING** - Indicates that a supplicant is being authenticated. • **AUTHENTICATED** - Indicates that the Authenticator has successfully authenticated the supplicant. • **ABORTING** - Indicates that the authentication procedure is being prematurely aborted due to the receipt of a re-authentication request, an EAPOL-Start frame, an EAPOL-Logoff frame, or an authentication timeout. • **HELD** - Indicates that the state machine ignores and discards all EAPOL packets in order to discourage brute force attacks. This state is entered from the AUTHENTICATING state following an authentication failure. • **FORCE_AUTH** - Indicates that the supplicant is always authorized. • **FORCE_UNAUTH** - Indicates that the supplicant is always unauthorized.
802.1X Backend State	Indicates the 802.1X backend PAE state. It can be one of the following values: • **REQUEST** - Indicates that the state machine has received an EAP request packet from the authentication server and is relaying that packet to the Supplicant as an EAPOL-encapsulated frame. • **RESPONSE** - Indicates that the state machine has received an EAPOL-encapsulated EAP Response packet from the supplicant and is relaying the EAP packet to the authentication Server. • **SUCCESS** - Indicates that the authentication server has confirmed that the supplicant is a legal client. The backend state machine will notify the authenticator PAE state machine and the supplicant. • **FAIL** - Indicates that the authentication server has confirmed the supplicant is an illegal client. The backend state machine will notify the authenticator PAE state machine and the supplicant. • **TIMEOUT** - Indicates that the authentication server or supplicant has time out. • **IDLE** - In this state, the state machine is waiting for the Authenticator state machine to signal the start of a new authentication session. • **INITIALIZE** - Indicates the authenticator is initializing the state machine.

47. Network Protocol Port Protection Commands

47-1 network-protocol-port protect

This command is used to enable the network protocol port protection function. Use the **no** form of this command to disable this function.

network-protocol-port protect {tcp | udp}

no network-protocol-port protect {tcp | udp}

Parameters

tcp	Specifies to protect the TCP port.
udp	Specifies to protect the UDP port.

Default

By default, this function is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the network protocol port protection function. If the port is protected, the Switch will not send any response packet to the closed TCP or UDP port.

Example

This example shows how to enable TCP port protection.

```
Switch# configure terminal
Switch(config)# network-protocol-port protect tcp
Switch(config)#
```

47-2 show network-protocol-port protect

This command is used to display the information of the network protocol port protection.

show network-protocol-port protect

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the information of the network protocol port protection.

Example

This example shows how to display the information of the network protocol port protection.

```
Switch# show network-protocol-port protect

     TCP Port protect state: Enabled
     UDP Port protect state: Enabled

Switch#
```

48. Packet Debug Commands

48-1 debug clear cpu counter

This command is used to clear packet counters including RX and TX of the CPU port.

debug clear cpu counter

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear packet counters including RX and TX of the CPU port and calculate again.

Example

This example shows how to clear packet counters of the CPU.

```
Switch#debug clear cpu counter

Success

Switch#
```

48-2 debug dump packet_in_buffer

This command is used to check received packets in buffer.

debug dump packet_in_buffer [len *LENGTH***][count** *COUNT***] [channel** *CHANNEL***]**

Parameters

len *LENGTH*	(Optional) Specifies the print buffer length of each packet in bytes. The value is from 1 to 2048.
count *COUNT*	(Optional) Specifies the packets count in each channel. The value is from 1 to 200.
channel *CHANNEL*	(Optional) Specifies the dump channel. The value is from 1 to 4.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

The command is used to check received packets in buffer. The system can buffer up to 200 packets per channel, and there are 3 channels in total for all packets. The system will prefer the lower position for the newer incoming packet. If the system is busy, the received packets will be buffered in the higher position. This can be used to check packets in the higher position for the CPU busy reason.

Example

This example shows how to dump packets in channel 2.

```
Switch#debug dump packet_in_buffer channel 2

#============================================================================
#ada69580-----------------------------------------------------------------
2019-01-01 00:02:41.506807 00 cnt 2, len 64,flags=4 port:1:1,DMA channel:2(FREE)
#>IP         ,EthRxNo    :  690,time:00000001(us,diff 1)
#>FreeMem    ,pkt_dbg.c  : 1331,time:00000102(us,diff 101)
0000: 00 57 a7 ad 10 01 f0 7d  68 12 10 01 81 00 80 01    .W.....}h.......
0010: 08 00 45 00 00 28 71 53  40 00 7f 06 c1 59 0a 5a    ..E..(qS@....Y.Z
0020: 5a 15 0a 5a 5a 5a c1 56  00 50 b6 60 8a 1f 01 e0    Z..ZZZ.V.P.`....
0030: a0 7d 50 10 3f 4a 02 e3  00 00                      .}P.?J....
#ada79780-----------------------------------------------------------------
2019-01-01 00:02:41.669789 01 cnt 2, len 64,flags=4 port:1:1,DMA channel:2(FREE)
#>IP         ,EthRxNo    :  756,time:00000002(us,diff 2)
#>FreeMem    ,pkt_dbg.c  : 1331,time:00000397(us,diff 395)
0000: 80 95 a6 ad 10 01 f0 7d  68 12 10 01 81 00 80 01    .......}h.......
0010: 08 00 45 00 00 28 71 95  40 00 7f 06 c1 17 0a 5a    ..E..(q.@......Z
0020: 5a 15 0a 5a 5a 5a c1 56  00 50 b6 60 8a 1f 01 e0    Z..ZZZ.V.P.`....
0030: e6 31 50 10 40 29 bc 4f  00 00                      .1P.@).O..
#============================================================================
#Allocate packet memory 0, print 2
#Use '%Y-%m-%d %H:%M:%S.' as timestamp format string to import to wireshark

Switch#
```

48-3 debug show cpu counter

This command is used to display packet counters including RX and TX of the CPU port.

debug show cpu counter

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is used to display packet counters including RX and TX of the CPU port.

Example

This example shows how display packet counters of the CPU port.

```
Switch#debug show cpu counter

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
----------- ------RX-TX------ --RX-TX-- ----------- ------RX-TX------ --RX-TX--
UNKNOWN            0-0           0-0    1X_BPDU            0-0           0-0
STP_BPDU           0-0           0-0    GVRP_BPDU          0-0           0-0
IP               485-341         0-0    LACP_BPDU          0-0           0-0
BPDU               0-0           0-0    ARP             1296-3           0-0
IPv6               0-0           0-0    CTP                0-0           0-0
LLDP               0-0           0-0    DDPv4              0-0           0-0
DDPv6              0-0           0-0    DDP_L2             0-0           0-0
Stacking           0-0           0-0    Total           1781-344         0-0









CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Display Parameters

PacketType	Received packets type of each protocol.
TotalCounter	Total received and transmitted counters of CPU port.
Pkt/Sec	RX or TX rate in packets per second.

49. Port Security Commands

49-1 clear port-security

This command is used to delete the auto-learned secured MAC addresses.

clear port-security {all | {address *MAC-ADDR* **| interface** *INTERFACE-ID* **[, | -]} [vlan** *VLAN-ID***]}**

Parameters

all	Specifies to delete all auto-learned secured entries.
address *MAC-ADDR*	Specifies to delete the specified auto -learned secured entry based on the MAC address entered.
interface *INTERFACE-ID*	Specifies to delete all auto-learned secured entries on the specified physical interface.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan *VLAN-ID*	Specifies to delete the auto-learned secured entry learned with the specified VLAN.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear auto-learned secured entries, either dynamic or permanent.

Example

This example shows how to remove a specific secure address from the MAC address table.

```
Switch#clear port-security address 0080.0070.0007
Switch#
```

49-2 show port-security

This command is used to display the current port security settings.

show port-security [interface *INTERFACE-ID* **[, | -]] [address]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
address	(Optional) Specifies to display all the secure MAC addresses, including both configured and learned entries.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the current port security settings.

Example

This example shows how to display the port security settings on ports 1 to 3.

```
Switch#show port-security interface eth1/0/1-3

 D:Delete-on-Timeout    P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.   No.     Act.       Count           Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 eth1/0/1     5     2     Restrict 0                    D  Enabled  Forwarding
 eth1/0/2     10    10    Shutdown 0                    D  Enabled  Err-disabled
 eth1/0/3     10    0     Shutdown 0                    P  Disabled -

Switch#
```

49-3 snmp-server enable traps port-security

This command is used to enable the sending of SNMP notifications for port security address violations. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps port-security [trap-rate *TRAP-RATE***]**

no snmp-server enable traps port-security [trap-rate]

Parameters

trap-rate *TRAP-RATE*	(Optional) Specifies the number of traps per second. The range is from 0 to 1000. The default value ("0") indicates an SNMP trap to be generated for every security violation.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for port security address violations and configure the number of traps per second.

Example

This example shows how to enable the sending of SNMP notifications for port security address violations and set the number of traps per second to 3.

```
Switch# configure terminal
Switch(config)#snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

49-4 switchport port-security

This command is used to configure the port security settings to restrict the number of users that are allowed to gain access rights to a port. Use the **no** form of this command to disable port security or to delete a secure MAC address.

switchport port-security [maximum *VALUE* **| violation {protect | restrict | shutdown} | mode {permanent | delete-on-timeout} | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

no switchport port-security [maximum | violation | mode | mac-address [permanent] *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

Parameters

maximum *VALUE*	(Optional) Specifies to set the maximum number of secure MAC addresses allowed. If not specified, the default value is 32. The valid range is from 0 to 64.
protect	(Optional) Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count.
restrict	(Optional) Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log.
shutdown	(Optional) Specifies to shut down the port if there is a security violation and record the system log.
permanent	(Optional) Specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries.
delete-on-timeout	(Optional) Specifies that under this mode, all learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries.
mac-address *MAC-ADDRESS*	(Optional) Specifies to add a secure MAC address to gain port access rights.
permanent	(Optional) Specifies to set the secure permanent configured MAC address of the port. This entry is same as the one learnt under the permanent mode.
vlan *VLAN-ID*	(Optional) Specifies a VLAN. If no VLAN is specified, the MAC address will be set with a PVID.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

When port security is enabled, if the port mode is configured as **delete-on-timeout**, the port will automatically learn the dynamic secured entry which will be timed out. These entries will be aged out based on the setting specified by the **switchport port-security aging** command. If the port mode is permanent, the port will automatically learn permanent secured entries which will not be timed out. The auto-learned permanent secured entry will be stored in the running configuration.

As the port mode-security state is changed, the violation counts will be cleared, and the auto-permanent entries will be converted to corresponding dynamic entries. As the port-security state is changed to disabled, the auto-learned secured entries, either dynamic or permanent with its violation counts are cleared. As the related VLAN configuration is changed, the auto-learned dynamic secured entries are cleared.

Permanent secured entry will be kept in the running configuration and can be stored to the NVRAM by using the **copy** command. The user configured secure MAC addresses are counted in the maximum number of MAC addresses on a port.

As a permanent secured entry of a port security enabled port, the MAC address cannot be moved to another port.

When the maximum setting is changed, the learned address will remain unchanged when the maximum number increases. If the maximum number is changed to a lower value which is lower than the existing entry number, the command is rejected.

A port-security enabled port has the following restrictions.

- The port security function cannot be enabled simultaneously with 802.1X and IMPB, that provides more advanced security capabilities.
- If a port is specified as the destination port for the mirroring function, the port security function cannot be enabled.
- If the port is a link aggregation member port, the port security function cannot be enabled.

When the maximum number of secured users is exceeded, one of the following actions can occur:

- **Protect** - When the number of port secure MAC addresses reaches the maximum number of users that is allowed on the port, the packets with the unknown source address is dropped until some secured entry is removed to release the space.
- **Restrict** - A port security violation restricts data and causes the security violation counter to increment.
- **Shutdown** - The interface is disabled, based on errors, when a security violation occurs.

Example

This example shows how to configure the port security mode to be permanent, specifying that a maximum of 5 secure MAC addresses are allowed on the port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security mode permanent
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)#
```

This example shows how to manually add the secure MAC addresses 00-00-12-34-56-78 with VID 5 on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

This example shows how to configure the Switch to drop all packets from the insecure hosts at the port-security process level and increment the security violation counter if a security violation is detected.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security violation restrict
Switch(config-if)#
```

49-5 switchport port-security aging

This command is used to configure the aging time for auto-learned dynamic secure addresses on an interface. Use the **no** form of this command to revert to the default settings.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**

no switchport port-security aging {time | type}

Parameters

time *MINUTES*	Specifies the aging time for the auto-learned dynamic secured address on this port. Its range is from 0 to 1440 in minutes.
type	Specifies to set the aging type.
absolute	Specifies to set absolute aging type. All the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type.
inactivity	Specifies to set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Default

By default, the port security aging feature is disabled.

The default time is 0 minutes.

The default aging type is **absolute**.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to disable the ageing or set the ageing time for auto-learned dynamic secured entries. In order for the inactivity setting to take effect, the FDB table ageing function must be enabled.

Example

This example shows how to apply the aging time for automatically learned secure MAC addresses on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security aging time 1
Switch(config-if)#
```

49-6 port-security limit

This command is used to configure the maximum secure MAC address number on the system. Use the **no** form of this command to revert to the default setting.

port-security limit global *VALUE*

no port-security limit global

Parameters

VALUE	Specifies the maximum number of port security entries that can be learned on the system. The range is from 1 to 1792. If the setting is smaller than the number of current learned entries, the command will be rejected.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to set the limit on the port security entry number which can be learned on a system.

Example

This example shows how to configure the maximum secure MAC address number for the system.

```
Switch# configure terminal
Switch(config)# port-security limit global 100
Switch(config)#
```

50. Power Saving Commands

50-1 dim led

This command is used to disable the port LED function. Use the **no** form of this command to revert to the default setting.

dim led

no dim led

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to turn off or turn on the port LED function. When the port LED function is disabled, LEDs used to illustrate port status are all turned off to save power.

Example

This example shows how to disable the port LED function.

```
Switch# configure terminal
Switch(config)# dim led
Switch(config)#
```

50-2 power-saving

This command is used to enable individual power saving functions. Use the **no** form of this command to disable these functions.

power-saving {link-detection | port-shutdown | dim-led | hibernation}

no power-saving {link-detection | port-shutdown | dim-led | hibernation}

Parameters

link-detection	Specifies that power saving will be applied by link status.
port-shutdown	Specifies that power saving will be applied by scheduled port shutdown.
dim-led	Specifies that power saving will be applied by scheduled dimming LEDs.
hibernation	Specifies that power saving will be applied by scheduled system hibernation.

Default

By default, all the options are disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable link detection, dimming LEDs, port shutdown, and hibernation using this command.

When link detection is enabled, the device can save power on the inactive ports.

When dim LED is enabled, the device will turn off all the port's LEDs in the specified time range to save power.

When port shutdown is enabled, the device will shut off all ports in the specified time range to save power.

When hibernation is enabled, the device will enter the hibernation mode in the specified time range to save power.

Example

This example shows how to enable power saving by shutting off the Switch's ports and toggle the Switch into the hibernation mode.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```

50-3 power-saving eee

This command is used to enable the Energy-Efficient Ethernet (EEE) function on the specified port(s). Use the **no** form of this command to disable the EEE function.

power-saving eee

no power-saving eee

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to enable or disable the specified port's EEE power saving function. The Energy-Efficient Ethernet (EEE) power-saving mode saves power consumption while a link is up when there is low utilization of packet traffic. The physical interface will enter into a Low Power Idle (LPI) mode when there is no data to be transmitted. In the EEE power-saving mode, power consumption is scalable to the actual bandwidth utilization.

Example

This example shows how to enable the EEE power saving function.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# power-saving eee
Switch(config-if)#
```

50-4 power-saving dim-led time-range

This command is used to configure the time range profile for the dim LED schedule. Use the **no** form of this command to delete the specified time range profile.

power-saving dim-led time-range *PROFILE-NAME*

no power-saving dim-led time-range *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the time range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to add or delete a time range profile for the dim LED schedule. When the schedule is up, all port LEDs will be turned off.

Example

This example shows how to add a time-range profile for the dim LED schedule.

```
Switch# configure terminal
Switch(config)# power-saving dim-led time-range off-duty
Switch(config)#
```

50-5 power-saving hibernation time-range

This command is used to configure the time range profile for the system hibernation schedule. Use the **no** form of this command to delete the specified time range profile.

power-saving hibernation time-range *PROFILE-NAME*

no power-saving hibernation time-range *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the time range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to add or delete a time range profile for the system hibernation schedule. When the system enters the hibernation mode, the Switch will go into a low power state and idle. It will shut down all the ports and LEDs, all network function will be disabled, and only the console connection will work via the RS232 port. If the Switch is an endpoint type Power Sourcing Equipment (PSE), the Switch will not provide power to the port.

Example

This example shows how to add a time range profile for the hibernation schedule.

```
Switch# configure terminal
Switch(config)# power-saving hibernation time-range off-duty
Switch(config)#
```

50-6 power-saving shutdown time-range

This command is used to configure the time range profile for the port shutdown schedule. Use the **no** form of this command to delete the specified time range profile.

power-saving shutdown time-range *PROFILE-NAME*

no power-saving shutdown time-range *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the time range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to add or delete a time range profile for the port shutdown schedule. When the schedule is up, the specific port will be disabled.

Example

This example shows how to add a time range profile for the port shutdown schedule.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# power-saving shutdown time-range off-duty
Switch(config-if)#
```

50-7 show power-saving

This command is used to display the power saving configuration information.

show power-saving [link-detection] [dim-led] [port-shutdown] [hibernation] [eee]

Parameters

link-detection	(Optional) Specifies to display the link detection state.
dim-led	(Optional) Specifies to display the dim LED state.
port-shutdown	(Optional) Specifies to display the port shutdown state.
hibernation	(Optional) Specifies to display the hibernation state.
eee	(Optional) Specifies to display the EEE state.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all power saving configuration information will be displayed.

Example

This example shows how to display all power saving configuration information.

```
Switch#show power-saving
Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

51. Protocol Independent Commands

51-1 ip route

This command is used to create a static route entry. Use the **no** form of this command to remove a static route entry.

ip route *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS* **[primary | backup]**

no ip route *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS*

Parameters

NETWORK-PREFIX	Specifies the network address.
NETWORK-MASK	Specifies the network mask.
IP-ADDRESS	Specifies the IP address of the next hop that can be used to reach destination network.
primary	(Optional) Specifies the route as the primary route to the destination.
backup	(Optional) Specifies the route as the backup route to the destination.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create an IP static route. Floating static route is supported. This means that there could be two routes with the same destination network address and different next hop. If **primary** or **backup** is not specified, the static route will be automatically determined to be a primary route or a backup route. Primary route has higher priority than backup route, and is always be used for forwarding when it is active. When primary is down, the backup route will be used.

Example

This example shows how to add a static route entry for 20.0.0.0/8 with the next-hop 10.1.1.254.

```
Switch#configure terminal
Switch(config)# ip route 20.0.0.0 255.0.0.0 10.1.1.254
Switch(config)#
```

51-2 ipv6 route

This command is used to create an IPv6 static route entry. Use the **no** form of this command to remove an IPv6 static route entry.

ipv6 route {default | *NETWORK-PREFIXIPREFIX-LENGTH***} [***INTERFACE-ID***]** *NEXT-HOP-ADDRESS* **[primary | backup]**

no ipv6 route {default | *NETWORK-PREFIXIPREFIX-LENGTH***} [***INTERFACE-ID***]** *NEXT-HOP-ADDRESS*

Parameters

default	Specifies to add or delete a default route.
NETWORK-PREFIX/PREFIX-LENGTH	Specifies the network prefix and the prefix length of the static route.
INTERFACE-ID	(Optional) Specifies the forwarding interface for routing the packet.
NEXT-HOP-ADDRESS	Specifies the IPv6 address of the next hop to reach the destination network. If the address is a link-local address, then the interface ID also need to be specified.
primary	(Optional) Specifies the route as the primary static route to the destination.
backup	(Optional) Specifies the route as the backup static route to the destination.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Floating static route is supported. This means that there could be two routes with same destination network address and different next hop. If **primary** or **backup** is not specified, the static route will be automatically determined to be a primary route or a backup route. Primary route has higher priority than backup route, and is always be used for forwarding when it is active. When primary is down, the backup route will be used.

Example

This example shows how to create a static route destined to the network where proxy server resides.

```
Switch#configure terminal
Switch(config)# ipv6 route 2001:0101::/32 vlan1 fe80::0000:00ff:1111:2233
Switch(config)#
```

51-3 show ip route

This command is used to display the entry in the routing table.

show ip route [*IP-ADDRESS* **[***MASK***] | connected | static | hardware]**

Parameters

IP-ADDRESS	(Optional) Specifies the network address of which routing information should be displayed.
MASK	(Optional) Specifies the subnet mask for the specified network.
connected	(Optional) Specifies to display directly connected route.
static	(Optional) Specifies to display the static route.
hardware	(Optional) Specifies to display the routes that have been written into chip.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the best routes that are currently at work.

Example

This example shows how to display the routing table.

```
Switch#show ip route
Code: C - connected, S - static
      * - candidate default


Gateway of last resort is 10.1.1.254 to network 0.0.0.0

S*   0.0.0.0/0 [1/1] via 10.1.1.254, vlan1
C    10.0.0.0/8 is directly connected, vlan1

Total Entries: 2


Switch#
```

51-4 show ip route summary

This command is used to display the brief information for the working routing entries.

show ip route summary

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the brief information for the working routing entries.

Example

This example shows how to display the brief information for the working routing entries.

```
Switch# show ip route summary

Route Source    Networks
Connected       1
Static          0
Total           1

Switch#
```

51-5 show ipv6 route

This command is used to display the entry in routing table.

show ipv6 route [[*IPV6-ADDRESS* **|** *NETWORK-PREFIX/PREFIX-LENGTH* **| interface** *INTERFACE-ID* **|** *PROTOCOL***] [database] | hardware]**

Parameters

IPV6-ADDRESS	(Optional) Specifies an IPv6 address to find a longest prefix matched IPv6 route.
NETWORK-PREFIX/ PREFIX-LENGTH	(Optional) Specifies the network address and prefix length of which routing information should be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the interface that will be used in the display.
PROTOCOL	(Optional) Specifies the routing protocol. It must be one of the following keywords: **static** and **connected**.
database	(Optional) Specifies to display all the related entries in the routing database instead of just the best route.
hardware	(Optional) Specifies to display the routes that have been written into chip.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the entry in routing table.

Example

This example shows how to display the routing entries for IPv6.

```
Switch#show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static
      SLAAC - Stateless address autoconfiguration

C     2000:410:1::/64 [0/1] is directly connected, vlan1
S     2001:0101::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1
S     2001:0102::/64 [1/1] via fe80::0000:00ff:1111:2233, vlan1

Total Entries: 3 entries, 3 routes
Switch#
```

51-6 show ipv6 route summary

This command is used to display the brief information for the working IPv6 routing entries.

show ipv6 route summary

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

When the system provides forwarding services for IPv6 traffic, it is very important and helpful to check the forwarding/routing table to understand what the traffic path will be currently in the network.

Example

This example shows how to display the brief information for the working IPv6 routing entries.

```
Switch#show ipv6 route summary

Route Source    Networks
Connected       2
Static          1
SLAAC           0
Total           3

Switch#
```

52. Quality of Service (QoS) Commands

52-1 class

This command is used to specify the name of the class map to be associated with a traffic policy and then enter into policy map class configuration mode. Use the **no** form of this command to remove the policy definition for the specified class.

class *NAME*

no class *NAME*

class class-default

Parameters

NAME	Specifies the name of the class map to be associated with a traffic policy.

Default

None.

Command Mode

Policy-map Configuration Mode.

Usage Guideline

Use this command to the Policy-map Configuration Mode. All the traffic that does not match the proceeding defined class will be classified as class-default. If the specified name of class map does not exist, no traffic is classified to the class.

Example

This example shows how to define a policy map, policy1, which defines policies for the class “class-dscp-red”. The packets that match DSCP 10, 12, or 14 will all be marked as DSCP 10.

```
Switch# configure terminal
Switch(config)# class-map class-dscp-red
Switch(config-cmap)# match ip dscp 10,12,14
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-dscp-red
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)#
```

52-2 class-map

This command is used to create or modify a class-map that defines the criteria for packet matching. Use the **no** form of this command to remove an existing class map from the Switch.

class-map [match-all | match-any] *NAME*

no class-map *NAME*

Parameters

match-all	(Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical AND. If neither **match-all** nor **match-any** is specified, **match-any** is implied.
match-any	(Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical OR. If neither **match-all** nor **match-any** is specified, **match-any** is implied.
NAME	Specifies the name of the class map with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create or modify a class-map that defines the criteria for matching packets. This command enters the Class-map Configuration Mode where match commands are entered to define the match criteria for this class.

When multiple match commands are defined for a class, use the **match-all** or **match-any** parameter to specify whether to evaluate the multiple match criteria based on either the logical AND or the logical OR.

Example

This example shows how to configure the “class_home_user “as the name of a class map. In this class map, a match statement specifies that the traffic that matches the access control list “acl_home_user” and matches the IPv6 protocol will be included under the class-map “class_home_user”.

```
Switch# configure terminal
Switch(config)# class-map match-all class_home_user
Switch(config-cmap)# match access-group name acl_home_user
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)#
```

52-3 match

This command is used to define the match criteria for a class-map. Use the **no** form of this command to remove the match criteria.

match {access-group name *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

no match {access-group name *ACCESS-LIST-NAME* **| cos** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan** *VLAN-ID-LIST***}**

Parameters

access-group name *ACCESS-LIST-NAME*	Specifies an access list to be matched. Traffic that is permitted by the access list will be classified.
cos *COS-LIST*	Specifies a specific IEEE 802.1Q CoS value(s) to be matched. The COS-LIST parameter values are from 0 to 7. Enter one or more CoS values separated by commas or hyphen for a range list.

[ip] dscp *DSCP-LIST*	Specifies differentiated service code point values to be matched. Enter one or more differentiated service code point (DSCP) values separated by commas or hyphen for a range list. The valid range is from 0 to 63. • **ip** - (Optional) Specifies that the match is for IPv4 packets only. If not specified, the match is for both IPv4 and IPv6 packets.
[ip] precedence *IP-PRECEDENCE-LIST*	Specifies IP precedence values to be matched. Enter one or more precedence values separated by commas or hyphen for a range list. The valid range is from 0 to 7. • **ip** - (Optional) Specifies that the match is for IPv4 packets only. If not specified, the match is for both IP and IPv6 packets. For IPv6 packets, the precedence is most three significant bits of traffic class of IPv6 header.
protocol *PROTOCOL-NAME*	Specifies the protocol name to be matched.
vlan *VLAN-ID-LIST*	Specifies the VLAN identification number, numbers, or range of numbers to be matched. Valid VLAN identification numbers must be in the range of 1 to 4094. Enter one or more VLAN values separated by commas or hyphens for a range list.

Default

None.

Command Mode

Class-map Configuration Mode.

Usage Guideline

To use the match command, first enter the class-map command to specify the name of the class that will be used to establish the match criteria. The policy for handling these matched packets is defined in the policy-map class configuration mode.

The following lists the reference for the supported protocols for the match protocol command.

- **arp** - IP Address Resolution Protocol (ARP).
- **bgp** - Border Gateway Protocol.
- **dhcp** - Dynamic Host Configuration.
- **dns** - Domain Name Server lookup.
- **egp** - Exterior Gateway Protocol.
- **ftp** - File Transfer Protocol.
- **ip** - IP (version 4).
- **ipv6** - IP (version 6).
- **netbios** - NetBIOS.
- **nfs** - Network File System.
- **ntp** - Network Time Protocol.
- **ospf** - Open Shortest Path First.
- **pppoe** - Point-to-Point Protocol over Ethernet.
- **rip** - Routing Information Protocol.
- **rtsp** - Real-Time Streaming Protocol.
- **ssh** - Secured shell.
- **telnet** - Telnet.
- **tftp** - Trivial File Transfer Protocol.

Example

This example shows how to specify a class map called “class-home-user” and configures the access list named “acl-home-user” to be used as the match criterion for that class.

```
Switch# configure terminal
Switch(config)# class-map class-home-user
Switch(config-cmap)# match access-group name acl-home-user
Switch(config-cmap)#
```

This example shows how to specify a class map called “cos” and specifies that the CoS values of 1, 2, and 3 are match criteria for the class.

```
Switch# configure terminal
Switch(config)# class-map cos
Switch(config-cmap)# match cos 1,2,3
Switch(config-cmap)#
```

52-4 mls qos cos

This command is used to configure the default Class of Service (CoS) value of a port. Use the **no** form of this command to revert to the default settings.

mls qos cos {*COS-VALUE* **| override}**

no mls qos cos

Parameters

COS-VALUE	Specifies to assign a default CoS value to a port. This CoS will be applied to the incoming untagged packets received by the port.
override	Specifies to override the CoS of the packets. The default CoS will be applied to all incoming packets, tagged or untagged, received by the port.

Default

By default, this CoS value is 0.

Command Mode

Interface Configuration Mode.

Usage Guideline

When the **override** parameter is not specified, the CoS of the packets will be the packet’s CoS if the packets are tagged, and will be the port default CoS if the packet is untagged.

When the **override** parameter is specified, the port default CoS will be applied to all packets received by the port. Use the **override** parameter when all incoming packets on certain ports deserve a higher or lower priority than packets that enter from other ports. Even if a port was previously set to trust DSCP or CoS, this command overrides that trust state, and all CoS values on the incoming packets are changed to the default CoS value that is configured with the **mls qos cos** command. If an incoming packet is tagged, the CoS value of the packet is modified at the ingress port.

Example

This example shows how to configure the default CoS value to 3 on port 1.

```
Switch# configure terminal
Switch(config)# interface  eth1/0/1
Switch(config-if)# mls qos cos 3
Switch(config-if)#
```

52-5 mls qos dscp-mutation

This command is used to attach an ingress Differentiated Services Code Point (DSCP) mutation map to the interface. Use the **no** form of this command to remove the ingress DSCP mutation map association from the interface.

mls qos dscp-mutation *DSCP-MUTATION-TABLE-NAME*

no mls qos dscp-mutation

Parameters

DSCP-MUTATION-TABLE-NAME	Specifies the name of the DSCP mutation table. The string of the name is up to 32 characters and no space is allowed.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to attach an ingress DSCP mutation table to an interface. The ingress DSCP mutation will mutate the DSCP value right after the packet is received by the interface, and QoS handles the packet with this new value. The Switch sends the packet out the port with the new DSCP value.

Example

This example shows how to map DSCP 30 to the mutated DSCP value 8 and attach the ingress-DSCP mutation map named “mutemap1” to port 1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos dscp-mutation mutemap1
Switch(config-if)#
```

52-6 mls qos map dscp-cos

This command is used to define a DSCP-to- CoS map. Use the **no** form of this command to revert to the default setting.

mls qos map dscp-cos *DSCP-LIST* **to** *COS-VALUE*

no mls qos map dscp-cos *DSCP-LIST*

Parameters

dscp-cos *DSCP-LIST* **to** *COS-VALUE*	Specifies the list of DSCP code points to be mapped to a CoS value. The range is from 0 to 63. The range is from 0 to 63. The series of DSCPs can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after.
DSCP-LIST	Specifies the range of DSCP values.

Default

CoS Value:	0	1	2	3	4	5	6	7
DSCP Value:	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63

Command Mode

Interface Configuration Mode.

Usage Guideline

The DSCP to CoS map is used by a DSCP trust port to map a DSCP value to an internal CoS value. In turn this CoS value is then mapped to the CoS queue based on the CoS to queue map configured by the **priority-queue cos-map** command.

Example

This example shows how to configure the DSCP to CoS map for mapping DSCP 12, 16, and 18 to CoS 1 on port 6.

```
Switch# configure terminal
Switch(config)# interface eth1/0/6
Switch(config-if)# mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

52-7 mls qos map dscp-mutation

This command is used to define a named DSCP mutation map. Use the **no** form of this command to remove the mutation map.

mls qos map dscp-mutation *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*

no mls qos map dscp-mutation *MAP-NAME*

Parameters

MAP-NAME	Specifies the name of the DSCP mutation map in a string length up to 32 characters (no space is allowed).
INPUT-DSCP-LIST	Specifies the list of DSCP code point to be mutated to another DSCP value. The range is from 0 to 63. The series of DSCPs can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after.
OUTPUT-DSCP	Specifies the mutated DSCP value. Valid values are from 0 to 63.

Default

The output DSCP is equal to the input DSCP.

Command Mode

Global Configuration Mode.

Usage Guideline

When a packet is received by an interface, based on a DSCP mutation map, the incoming DSCP can be mutated to another DSCP immediately before any QoS operations. The DSCP mutation is helpful to integrate domains with different DSCP assignments.

When configuring a named DSCP mutation map, note the following:

- Enter multiple commands to map additional DSCP values to a mutated DSCP value.
- Enter a separate command for each mutated DSCP value.

The DSCP-CoS map will still be based on the packet's original DSCP. All the subsequent operations will base on the mutated DSCP.

Example

This example shows how to map DSCP 30 to the mutated DSCP value 8, DSCP 20 to the mutated DSCP 10, with the mutation map named "mutemap1".

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# mls qos map dscp-mutation mutemap1 20 to 10
Switch(config)#
```

52-8 mls qos scheduler

This command is used to configure the scheduling mechanism. Use the **no** form of this command to revert to the default setting.

mls qos scheduler {sp | rr | wrr | wdrr}

no mls qos scheduler

Parameters

sp	Specifies that all queues are in Strict Priority (SP) scheduling.
rr	Specifies that all queues are in Round-Robin (RR) scheduling.
wrr	Specifies the queues in the frame count Weighted Round-Robin (WRR) scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode.
wdrr	Specifies the queues of all ports in the frame length (quantum) Weighted Deficit Round-Robin (WDRR) scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode.

Default

The default queue scheduling algorithm is WRR.

Command Mode

Interface Configuration Mode.

Usage Guideline

Specify schedule algorithms to WRR, SP, RR or WDRR for the output queue. By default, the output queue scheduling algorithm is WRR. WDRR operates by serving an accumulated set of backlogged credits in the transmit

queue in a round robin order. Initially, each queue sets its credit counter to a configurable quantum value. Every time a packet from a CoS queue is sent, the size of the packet is subtracted from the corresponding credit counter and the service right is turned over to the next lower CoS queue. When the credit counter drops below 0, the queue is no longer serviced until its credits are replenished. When the credit counters of all CoS queues reaches 0, the credit counters will be replenished at that time.

All packets are serviced until their credit counter is zero or negative and the last packet is transmitted completely. When this condition happens, the credits are replenished. When the credits are replenished, a quantum of credits are added to each CoS queue credit counter. The quantum for each CoS queue may be different based on the user configuration.

To set a CoS queue in the strict priority mode, any higher priority CoS queue must also be in the strict priority mode.

WRR operates by transmitting permitted packets into the transmit queue in a round robin order. Initially, each queue sets its weight to a configurable weighting. Every time a packet from a higher priority CoS queue is sent, the corresponding weight is subtracted by 1, and the packet in the next lower CoS queue will be serviced. When the weight of a CoS queue reaches zero, the queue will not be serviced until its weight is replenished. When weights of all CoS queues reach 0, the weights get replenished at a time.

Example

This example shows how to configure the queue scheduling algorithm to the strict priority mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos scheduler sp
Switch(config-if)#
```

52-9 mls qos trust

This command is used to configure the trust state of a port to trust either the CoS field or the DSCP field of the arriving packet for subsequent QoS operation. Use the **no** form of this command to revert to the default setting.

mls qos trust {cos | dscp}

no mls qos trust

Parameters

cos	Specifies that the CoS bits of the arriving packets are trusted for subsequent QoS operations.
dscp	Specifies that the ToS/DSCP bits, if available in the arriving packets, are trusted for subsequent operations. For non-IP packet, Layer 2 CoS information will be trusted for traffic classification.

Default

By default, CoS is trusted.

Command Mode

Interface Configuration Mode.

Usage Guideline

When the interface is set to trust DSCP, the DSCP of the arriving packet will be trusted for the subsequent QoS operations. First, the DSCP will be mapped to an internal CoS value, which will be subsequently used to determine the CoS queue. The DSCP to CoS map is configured by the **mls qos map dscp-cos** command. The CoS to queue map is configured by the **priority-queue cos-map** command. If the arriving packet is a non-IP packet, the CoS is trusted. The resulting CoS mapped from DSCP will also be the CoS in the transmitted packet.

When an interface is in the trust CoS state, the CoS of the arriving packet will be applied to the packet as the internal CoS and used to determine the CoS queue. The CoS queue is determined based on the CoS to Queue mapping table.

When a packet arrives at an 802.1Q VLAN tunnel port, the packet will be added with an outer VLAN tag in order to transmit through the VLAN tunnel. If the port is to trust CoS, then the inner tag CoS will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag. If the MLS QoS CoS override is configured, then the CoS specified by command mls qos cos will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag. If the port is to trust DSCP, then the CoS mapped from the DSCP code point will be the internal CoS of the packet and the CoS value in the packet's outer VLAN tag

Example

This example shows how to configure port 1 to trust the DSCP mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)#
```

52-10 policy-map

This command is used to enter the Policy-map Configuration Mode, and create or modify a policy map that can be attached to one or more interfaces as a service policy. Use the **no** form of this command to delete a policy map.

policy-map *NAME*

no policy-map *NAME*

Parameters

NAME	Specifies the name of the policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the Policy-map Configuration Mode from where the user can configure or modify the policy for the traffic class. A single policy map can be attached to more than one interface concurrently. The succeeding policy-map attaches overwrite the previous one.

Policy maps contain traffic classes. Traffic classes contain one or more match commands that can be used to match packets (and organize them into groups) on the basis of a protocol type or application.

Example

This example shows how to create a policy map called policy and configures two class policies within the policy map. The class policy called class1 specifies a policy for traffic that matches an ACL “acl_rd”. The second class is the default class, named class-default to include packets that do not match the defined classes.

```
Switch# configure terminal
Switch(config)# class-map class1
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# exit
Switch(config)# policy-map policy
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 46
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set ip dscp 00
Switch(config-pmap-c)#
```

52-11 priority-queue cos-map

This command is used to used to define a CoS to queue map. Use the **no** form of this command to revert to the default setting.

priority-queue cos-map QUEUE-ID *COS1* **[***COS2* **[***COS3* **[***COS4* **[***COS5* **[***COS6* **[***COS7* **[***COS8***]]]]]]]**

no priority-queue cos-map

Parameters

QUEUE-ID	Specifies the queue ID the CoS will be mapped.
COS1	Specifies the mapping CoS value. Valid values are from 0 to 7.
COS2…COS8	(Optional) Specifies the mapping CoS value. Valid values are from 0 to 7.

Default

The default priority (CoS) to queue mapping is: 0 to 2, 1 to 0, 2 to 1, 3 to 3, 4 to 4, 5 to 5, 6 to 6, 7 to 7.

Command Mode

Global Configuration Mode.

Usage Guideline

When a packet is received, the packet will be given an internal CoS. This internal CoS is used to select the transmit queue based on the CoS to queue map. The CoS queue with a higher number will receive a higher priority.

Example

This example shows how to assign CoS priority 3, 5 and 6 to queue 2.

```
Switch# configure terminal
Switch(config)# priority-queue cos-map 2 3 5 6
Switch(config)#
```

52-12 queue rate-limit

This command is used to specify or modify the bandwidth allocated for a queue. Use the **no** form of this command to remove the bandwidth allocated for a queue.

queue *QUEUE-ID* **rate-limit {***MIN-BANDWIDTH-KBPS* **| percent** *MIN-PERCENTAGE***} {***MAX-BANDWIDTH-KBPS* **| percent** *MAX-PERCENTAGE***}**

no queue *QUEUE-ID* **rate-limit**

Parameters

QUEUE-ID	Specifies the queue ID to set minimal guaranteed and maximum bandwidth.
MIN-BANDWIDTH-KBPS	Specifies the minimal guaranteed bandwidth in kilobits per second allocated to a specified queue.
MAX-BANDWIDTH-KBPS	Specifies the maximum bandwidth in kilobits per second for a specified queue.
MIN-PERCENTAGE	Specifies to set the minimal bandwidth by percentage. The valid range is from 1 to 100.
MAX-PERCENTAGE	Specifies to set the maximum bandwidth by percentage. The valid range is from 1 to 100.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure the minimal and maximum bandwidth for a specified queue. When the minimal bandwidth is configured, the packet transmitted from the queue can be guaranteed. When the maximum bandwidth is configured, packets transmitted from the queue cannot exceed the maximum bandwidth even if the bandwidth is available.

When configuring the minimal bandwidth, the aggregate of the configured minimum bandwidth must be less than 75 percent of the interface bandwidth to make sure the configured minimal bandwidth can be guaranteed. It is not necessary to set the minimum guaranteed bandwidth for the highest strict priority queue. This is because the traffic in this queue will be serviced first if the minimal bandwidth of all queues is satisfied.

The configuration of this command can only be attached to a physical port but not a port-channel. That is the minimum guaranteed bandwidth of one CoS cannot be used across physical ports.

Example

This example shows how to configure the queue bandwidth, the minimum guaranteed bandwidth and maximum bandwidth of queue 1 of port 1 to 100Kbps and 2000Kbps respectively. Set the minimum guaranteed bandwidth and maximum bandwidth of queue 2 to 10% and 50% respectively.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# queue 1 rate-limit 100 2000
Switch(config-if)# queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

52-13 rate-limit {input | output}

This command is used to set the received or transmitted bandwidth limit values for an interface. Use the **no** form of this command to disable the bandwidth limit.

rate-limit {input | output} {*NUMBER-KBPS* **| percent** *PERCENTAGE*} [*BURST-SIZE*]

no rate-limit {input | output}

Parameters

input	Specifies the bandwidth limit for ingress packets.
output	Specifies the bandwidth limit for egress packets.
NUMBER-KBPS	Specifies the number of kilobits per second as the maximum bandwidth limit.
PERCENTAGE	Specifies to set the limited rate by percentage. The valid range is 1 to 100.
BURST-SIZE	(Optional) Specifies the limit for burst traffic in Kbyte.

Default

By default, there is no limitation.

Command Mode

Interface Configuration Mode.

Usage Guideline

The specified limitation cannot exceed the maximum speed of the specified interface. For the ingress bandwidth limitation, the ingress will send a pause frame or a flow control frame when the received traffic exceeds the limitation.

Example

This example shows how to configure the maximum bandwidth limits on port 5. The ingress bandwidth is limited to 2000Kbps and 4096K bytes for burst traffic.

```
Switch# configure terminal
Switch(config)# interface eth1/0/5
Switch(config-if)# rate-limit input 2000 4096
Switch(config-if)#
```

52-14 service-policy

This command is used to attach a policy map to an input or output interface. Use the **no** form of this command to remove a service policy from an input or output interface.

service-policy {input | output} *NAME*

no service-policy {input | output}

Parameters

input	Specifies to apply the policy map for ingress flow on the interface.
output	Specifies to apply the policy map for egress flow on the interface.
NAME	Specifies the name of a service policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to attach at most one policy map for each type (input or output) on an interface. This policy is attached to the interface for aggregate and controls the number or rate of packets. A packet arriving at a port will be treated based on the service policy attached to the interface.

Example

This example shows how to create a policy map “cust1-class” and attach to port 1 for ingress traffic.

```
Switch#configure terminal
Switch(config)#policy-map cust1-classes
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#
```

52-15 set

This command is used to configure the new precedence field, DSCP field, and CoS field of the outgoing packet. The user can also specify the CoS queue for the packet. Use the **no** form of this command to remove the set.

set {[ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

no set {[ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

Parameters

precedence *PRECEDENCE*	Specifies a new precedence for the packet. The range is from 0 to 7. If the optional keyword ip is specified, IPv4 precedence will be marked. If not specified, both IPv4 and IPv6 precedence will be marked. For IPv6 packets, the precedence is the most three significant bits of traffic class of IPv6 header. Setting the precedence will not affect the CoS queue selection.
dscp *DSCP*	Specifies a new DSCP for the packet. The range is from 0 to 63. If the optional keyword ip is specified, IPv4 DSCP will be marked. If not specified, both IPv4 and IPv6 DSCP will be marked. Setting DSCP will not affect the CoS queue selection.
cos *COS*	Specifies to assign a new CoS value to the packet. The range is from 0 to 7.
cos-queue *COS-QUEUE*	Specifies to assign the CoS queue to the packets. This overwrites the original CoS queue selection.

Default

None.

Command Mode

Policy-map Class Configuration Mode.

Usage Guideline

Use this command to set the DSCP field, CoS field, or precedence field of the matched packet to a new value. Use the set cos-queue command to directly assign the CoS queue to the matched packets.

Configure multiple set commands for a class if they are not conflicting.

The set dscp command will not affect the CoS queue selection. The set cos-queue command will not alter the CoS field of the outgoing packet.

Example

This example shows how to configure the policy map “policy1” with the policy for the class1 class. The packets that are included in the class1 class will be set to a DSCP of 10.

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# set ip dscp 10
Switch(config-pmap-c)#
```

52-16 show class-map

This command is used to display the class map configuration.

show class-map [*NAME***]**

Parameters

NAME	(Optional) Specifies the name of the class map. The class map name can be a maximum of 32 alphanumeric characters.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display all class maps and their matching criteria.

Example

This example shows how to define two class maps. Packets that match the access list “acl_home_user” belong to the class “c3”, IP packets belong to the class “c2”.

```
Switch# show class-map

Class Map match-any class-default
   Match any

 Class Map match-all c2
   Match protocol ip

Class Map match-all c3
   Match access-group acl_home_user

Switch#
```

52-17 show mls qos interface

This command is used to display port level QoS configurations.

show mls qos interface [*INTERFACE-ID* **[, | -]] {cos | scheduler | trust | rate-limit | queue-rate-limit | dscp-mutation | map {dscp-cos}}**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
cos	Specifies to display the port default CoS.
scheduler	Specifies to display the transmit queue scheduling settings.
trust	Specifies to display the port trust State.
rate-limit	Specifies to display the bandwidth limitation configured for the port.
queue-rate-limit	Specifies to display the bandwidth allocation configured for the queue.
dscp-mutation	Specifies to display the DSCP mutation map attached to the interface.
map dscp-cos	Specifies to display the mapping of DSCP to CoS

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, the summary of QoS is displayed.When using the **rate-limit** or **queue-rate-limit** parameter to display, the information is displayed by percentage and actual rate if the port link is up, and the information is displayed by percentage if the port link is down.

Example

This example shows how to display the default CoS for ports 2 to 5.

```
Switch#show mls qos interface eth1/0/2-5 cos

 Interface     CoS   Override
 ------------  ----  ---------
 eth1/0/2      3     Yes
 eth1/0/3      4     No
 eth1/0/4      4     No
 eth1/0/5      3     No

Switch#
```

This example shows how to display the port trust state for ports 2 to 5.

```
Switch#show mls qos interface eth1/0/2-5 trust

 Interface     Trust State
 ------------  ------------
 eth1/0/2      trust DSCP
 eth1/0/3      trust CoS
 eth1/0/4      trust DSCP
 eth1/0/5      trust CoS

Switch#
```

This example shows how to display the scheduling configuration for ports 1 to 2.

```
Switch#show mls qos interface eth1/0/1-2 scheduler

 Interface     Scheduler Method
 ------------  -----------------
 eth1/0/1      sp
 eth1/0/2      wrr

Switch#
```

This example shows how to display the DSCP mutation maps attached to ports 1 to 2.

```
Switch#show mls qos interface eth1/0/1-2 dscp-mutation

 Interface     DSCP Mutation Map
 ------------  --------------------
 eth1/0/1      Mutate Map 1
 eth1/0/2      Mutate Map 2

Switch#
```

This example shows how to display the bandwidth allocation for ports 1 to 4.

```
Switch#show mls qos interface eth1/0/1-4 rate-limit

 Interface Rx Rate             TX Rate             Rx Burst       Tx Burst
 --------- ------------------- ------------------- -------------- -------------
 eth1/0/1  1000 kbps           No Limit            64 kbyte       No Limit
 eth1/0/2  No Limit            2000 kbps           No Limit       2000 kbyte
 eth1/0/3  10%(100000 kbps)    20%(200000 kbps)    64 kbyte       64 kbyte
 eth1/0/4  2%                  2000 kbps           64 kbyte       64 kbyte

Switch#
```

This example shows how to display the CoS bandwidth allocation for port 1.

```
Switch#show mls qos interface Ethernet 1/0/1 queue-rate-limit


eth1/0/1
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     No Limit             No Limit
 1     64 kbps              10%
 2     128 kbps             25600 kbps
 3     2%                   50%
 4     No Limit             No Limit
 5     No Limit             No Limit
 6     No Limit             No Limit
 7     No Limit             No Limit

Switch#
```

This example shows how to display the DSCP to CoS map for port 1.

```
Switch#show mls qos interface eth1/0/1 map dscp-cos

eth1/0/1
       0  1  2  3  4  5  6  7  8  9
     --------------------------------
   00  00 00 00 00 00 00 00 00 01 01
   10  01 01 01 01 01 01 02 02 02 02
   20  02 02 02 02 03 03 03 03 03 03
   30  03 03 04 04 04 04 04 04 04 04
   40  05 05 05 05 05 05 05 05 06 06
   50  06 06 06 06 06 06 07 07 07 07
   60  07 07 07 07


Switch#
```

52-18 show mls qos map dscp-mutation

This command is used to display the QoS DSCP mutation map configuration.

show mls qos map dscp-mutation [*MAP-NAME***]**

Parameters

MAP-NAME	(Optional) Specifies the name of the DSCP mutation map to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the QoS DSCP mutation map configuration.

Example

This example shows how to display the global DSCP mutation map.

```
Switch# show mls qos map dscp-mutation

DSCP Mutation: mutemap1
Attaching interface:
   eth1/0/3

       0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 01 02 03 04 05 06 07 08 09
   10  10 11 12 13 14 15 16 17 18 19
   20  20 21 22 23 24 25 26 27 28 29
   30  08 31 32 33 34 35 36 37 38 39
   40  40 41 42 43 44 45 46 47 48 49
   50  50 51 52 53 54 55 56 57 58 59
   60  60 61 62 63


Switch#
```

52-19 show mls qos queueing

This command is used to display the QoS queueing information and weight configuration for different scheduler algorithm on specified interface(s).

show mls qos queueing [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the QoS queueing information and weight configuration for different scheduler algorithm on specified interface(s). If no parameter is specified, the system-wide map of CoS to queue ID will be displayed.

The scheduling mode which is configured by the **mls qos scheduler** command determines which weight configuration taking effect. Use the **show mls qos interface scheduler** command to get the scheduling mode of an interface.

Example

This example shows how to display the QoS queueing information.

```
Switch# show mls qos queueing

 CoS-queue map:
   CoS   QID
   ---   ---
    0     2
    1     0
    2     1
    3     3
    4     4
    5     5
    6     6
    7     7

Switch#
```

This example shows how to display the weight configuration for the different scheduler on port 3.

```
Switch# show mls qos queueing interface eth1/0/3

wrr bandwidth weights:
  QID  Weights
  ---  -------
   0      1
   1      2
   2      3
   3      4
   4      5
   5      6
   6      7
   7      8

wdrr bandwidth weights:
  QID  Quantum
  ---  -------
   0      1
   1      2
   2      3
   3      4
   4      5
   5      6
   6      7
   7      8

Switch#
```

52-20 show policy-map

This command is used to display the policy map configuration.

show policy-map [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the policy map. If not specified, all policy maps will be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the physical port interface to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the class policy configured for the policy map.

Example

This example shows how to display the class policy configured for the policy map.

```
Switch#show policy-map

 Policy Map cust1-classes
  Class Map gold


Switch#
```

52-21 wdrr-queue bandwidth

This command is used to set the queue quantum in the WDRR scheduling mode. Use the **no** form of this command to revert to the default setting.

wdrr-queue bandwidth *QUANTUM1…QUANTUM8*

no wdrr-queue bandwidth

Parameters

QUANTUM1 …QUANTUM8	Specifies the quantum value (frame length count) for each of the eight quantum queues used in WDRR scheduling. The quantum value range is from 0 to 127.

Default

By default, the quantum value is 1 for all queues.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command takes effect when the scheduling mode is in the WDRR mode. Use the **mls qos scheduler wdrr** command to change the scheduling mode to the WDRR mode.

Example

This example shows how to configure the queue quantum of the WDRR scheduling mode, queue quantum of queue 0, queue 1, queue 2, queue 3, queue 4, queue 5, queue 6, queue 7 are 1, 2, 3, 4, 5, 6, 7, 8 respectively on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos scheduler wdrr
Switch(config-if)# wdrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

52-22 wrr-queue bandwidth

This command is used to set the queue weight in the WRR scheduling mode. Use the **no** form of this command to revert to the default setting.

wrr-queue bandwidth *WEIGHT1…WEIGHT8*

no wrr-queue bandwidth

Parameters

WEIGHT1 …WEIGHT8	Specifies the weight value (frame count) for each of the eight weight queues used in WRR scheduling. The weight value range is from 0 to 127.

Default

By default, the weight value for WEIGHT1 to WEIGHT7 is 1.

By default, the weight value for WEIGHT8 is 0.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command takes effect when the scheduling mode is in the WDRR mode. Use the **mls qos scheduler wdrr** command to change the scheduling mode to the WDRR mode. To meet the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So, the weight of the last queue should be zero while the Differentiate Service is supported.

Example

This example shows how to configure the queue weight of the WRR scheduling mode, queue weight of queue 0, queue 1, queue 2, queue 3, queue 4, queue 5, queue 6, queue 7 are 1, 2, 3, 4, 5, 6, 7, 8 respectively on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

53. Remote Network MONitoring (RMON) Commands

53-1 rmon collection stats

This command is used to enable RMON statistics on the configured interface. Use the **no** form of this command to disable the RMON statistics.

rmon collection stats *INDEX* **[owner** *NAME***]**

no rmon collection stats *INDEX*

Parameters

INDEX	Specifies the Remote Network Monitoring (RMON) table index. The range is from 1 to 65535.
owner *NAME*	Specifies the owner string. The maximum length is 127.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

The RMON statistics group entry number is dynamic. Only the interface that is enabled for RMON statistics will have a corresponding entry in the table.

Example

This example shows how to configure an RMON statistics entry with an index of 65 and the owner name “guest” on port 2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# rmon collection stats 65 owner guest
Switch(config-if)#
```

53-2 rmon collection history

This command is used to enable RMON MIB history statistics gathering on the configured interface. Use the **no** form of this command to disable history statistics gathering on the interface.

rmon collection history *INDEX* **[owner** *NAME***] [buckets** *NUM***] [interval** *SECONDS***]**

no rmon collection history *INDEX*

Parameters

INDEX	Specifies the history group table index. The range is from 1 to 65535.
owner *NAME*	Specifies the owner string. The maximum length is 127.

buckets *NUM*	Specifies the number of buckets specified for the RMON collection history group of statistics. If not specified, the default is 50. The range is from 1 to 65535.
interval *SECONDS*	Specifies the number of seconds in each polling cycle. The range is from 1 to 3600.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

The RMON history group entry number is dynamic. Only the interface that is enabled for RMON history statistics gathering will have a corresponding entry in the table. The configured interface becomes the data source for the created entry.

Example

This example shows how to enable the RMON MIB history statistics group on port 8.

```
Switch# configure terminal
Switch(config)# interface eth1/0/8
Switch(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

53-3 rmon alarm

This command is used to configure an alarm entry to monitor an interface. Use the **no** form of this command to remove an alarm entry.

rmon alarm *INDEX VARIABLE INTERVAL* **{delta | absolute} rising-threshold** *VALUE* **[***RISING-EVENT-NUMBER***] falling-threshold** *VALUE* **[***FALLING-EVENT-NUMBER***] [owner** *STRING***]**

no rmon alarm *INDEX*

Parameters

INDEX	Specifies the alarm index. The range is from 1 to 65535.
VARIABLE	Specifies the object identifier of the variable to be sampled.
INTERVAL	Specifies the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483647.
delta	Specifies that the delta of two consecutive sampled values is monitored.
absolute	Specifies that the absolute sampled value is monitored.
rising-threshold *VALUE*	Specifies the rising threshold. The valid range is from 0 to 2147483647.
RISING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the rising threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the ringing threshold.
falling-threshold *VALUE*	Specifies the falling threshold. The valid range is from 0 to 2147483647.
FALLING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.

owner *STRING*	Specifies the owner string. The maximum length is 127.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The RMON alarm facility periodically takes samples of the value of variables and compares them against the configured threshold.

Example

This example shows how to configure an alarm entry to monitor an interface.

```
Switch# configure terminal
Switch(config)# rmon alarm 783 1.3.6.1.2.1.2.2.1.12.6 30 delta rising-threshold 20 1 falling-threshold 10 1 owner Name
Switch(config)#
```

53-4 rmon event

This command is used to configure an event entry. Use the **no** form of this command to remove an event entry.

rmon event *INDEX* **[log] [[trap** *COMMUNITY***] [owner** *NAME***] [description** *STRING***]**

no rmon event *INDEX*

Parameters

INDEX	Specifies the index of the alarm entry. The valid range is from 1 to 65535.
log	(Optional) Specifies to generate log message for the notification.
trap *COMMUNITY*	(Optional) Specifies to generate SNMP trap messages for the notification. The maximum length is 127.
owner *NAME*	(Optional) Specifies the owner string. The maximum length is 127.
description *STRING*	(Optional) Specifies a description for the RMON event entry. Enter a text string with a maximum length of 127 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

If the **log** parameter is specified but not the **trap** parameter, the created entry will cause a log entry to be generated on an event occurrence. If the **trap** parameter is specified but not the **log** parameter, the created entry will cause an SNMP notification to be generated on an event occurrence.

If both **log** and **trap** are specified, the created entry will cause both the log entry and the SNMP notification to be generated on event occurrence.

Example

This example shows how to configure an event with an index of 13 to generate a log on the occurrence of the event.

```
Switch# configure terminal
Switch(config)# rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
Switch(config)#
```

53-5 show rmon alarm

This command is used to display the alarm configuration.

show rmon alarm

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the RMON alarm table.

Example

This example shows how to display the RMON alarm table.

```
Switch# show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

53-6 show rmon events

This command is used to display the RMON event table.

show rmon events

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the RMON event table.

Example

This example shows how to display the RMON event table.

```
Switch# show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2020-03-12

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time: 0:0:0, 0

Switch#
```

53-7 show rmon history

This command is used to display RMON history statistics information.

show rmon history

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the history of the statistics for all of the configured entries.

Example

This example shows how to display RMON Ethernet history statistics.

```
Switch# show rmon history

Index 23, owned by Manager, Data source is eth1/0/2
  Interval: 30 seconds
  Requested buckets: 50, Granted buckets: 50
  Sample #1
    Received octets: 303595962, Received packets: 357568
    Broadcast packets: 3289, Multicast  packets: 7287
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Sample #2
    Received octets: 303596354, Received packets: 357898
    Broadcast packets: 3329, Multicast  packets: 7337
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0

Switch#
```

53-8 show rmon statistics

This command is used to display RMON Ethernet statistics.

show rmon statistics

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display RMON Ethernet statistics.

Example

This example shows how to display RMON Ethernet statistics.

```
Switch# show rmon statistics

Index 32, owned by it@domain.com, Data Source is  eth1/0/3
  Received Octets : 234000, Received packets : 9706
  Broadcast packets: 2266, Multicast packets: 192
  Undersized packets: 213, Oversized  packets: 24
  Fragments: 2, Jabbers: 1
  CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Packets in 64 octets: 256, Packets in 65-127 octets : 236
  Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
  Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

53-9 snmp-server enable traps rmon

This command is used to enable the sending of SNMP notifications for RMON. Use the **no** form of this command to disable the sending of SNMP notifications for RMON.

snmp-server enable traps rmon [rising-alarm | falling-alarm]

no snmp-server enable traps rmon [rising-alarm | falling-alarm]

Parameters

rising-alarm	(Optional) Specifies to configure the rising alarm trap state.
falling-alarm	(Optional) Specifies to configure the falling alarm trap state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for RMON.

Example

This example shows how to enable the sending of RMON traps for both the falling alarm and rising alarm.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps rmon
Switch(config)#
```

54. Router Advertisement (RA) Guard Commands

54-1 ipv6 nd raguard policy

This command is used to create an RA guard policy. The command will enter into the RA Guard Policy Configuration Mode mode. Use the **no** form of this command to remove an RA guard policy.

ipv6 nd raguard policy *POLICY-NAME*

no ipv6 nd raguard policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the IPv6 RA guard policy name.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create or remove an RA guard policy. This command will enter the RA Guard Policy Configuration Mode.

Example

This example shows how to create an RA guard policy named policy1.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy policy1
Switch(config-ra-guard)#
```

54-2 device-role

This command is used to configure the role of the attached device. Use the **no** form of this command to revert to the default setting.

device-role {host | router}

no device-role

Parameters

host	Specifies to set the role of the attached device to host.
router	Specifies to set the role of the attached device to router.

Default

By default, this option is **host**.

Command Mode

RA Guard Policy Configuration Mode.

Usage Guideline

Use this command to set the role of the attached device. By default, the device role is **host**, and all the inbound router advertisement and redirect messages are blocked. If the device role is set to **router**, all messages, Router Solicitation (RS), Router Advertisement (RA), or redirect are allowed on this port.

Example

This example shows how to create an RA guard policy named “raguard1” and set the device as **host**.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# device-role host
Switch(config-ra-guard)#
```

54-3 match ipv6 access-list

This command is used to filter the RA messages based on the sender IPv6 address. Use the **no** form of this command to disable the filtering.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*

no match ipv6 access-list

Parameters

IPV6-ACCESS-LIST-NAME	Specifies a standard IPv6 access list.

Default

None.

Command Mode

RA Guard Policy Configuration Mode

Usage Guideline

Use this command to filter RA messages based on the sender IP address when the interface device role is set to **router**. If the **match ipv6 access-list** command is not configured, all RA messages are bypassed. An access list is configured using the **ipv6 access-list** command.

Example

This example shows how to create an RA guard policy and matches the IPv6 addresses in the access list named list1.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# match ipv6 access-list list1
Switch(config-ra-guard)#
```

54-4 ipv6 nd raguard attach-policy

This command is used to apply an RA guard policy on a specified interface. Use the **no** form of this command to remove the binding.

ipv6 nd raguard attach-policy [*POLICY-NAME***]**

no ipv6 nd raguard

Parameters

POLICY-NAME	(Optional) SSpecifies the IPv6 RA guard policy name.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

Only one RA policy can be attached. If no parameter is specified, the default policy will set the device role to **host**.

Example

This example shows how to apply the RA guard policy on port 3.

```
Switch# configure terminal
Switch(config)# ipv6 nd raguard policy raguard1
Switch(config-ra-guard)# device-role router
Switch(config-ra-guard)# match ipv6 access-list list1
Switch(config-ra-guard)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

54-5 show ipv6 nd raguard policy

This command is used to display RA guard policy information.

show ipv6 nd raguard policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) SSpecifies the IPv6 RA guard policy name.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display RA guard policy information. If no parameter is specified, information of all policies will be displayed for all policies.

Example

This example shows how to display the information of the RA guard policy “raguard1”.

```
Switch# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
      Device Role: host
      Target: eth1/0/1-1/0/2

Switch#
```

55. Safeguard Engine Commands

55-1 clear cpu-protect counters

This command is used to clear the CPU protect related counters.

clear cpu-protect counters {all | sub-interface [manage | protocol | route] | type [*PROTOCOL-NAME***]}**

Parameters

all	Specifies to clear all CPU protect counters.
sub-interface [manage | protocol | route]	Specifies to clear the CPU protect related counters of sub-interfaces. If no sub-interface is specified then the CPU protect related counters of all sub-interfaces will be cleared.
type [*PROTOCOL-NAME***]**	Specifies to clear the CPU protect related counters of the specified protocol. If no protocol name is specified, then all protocols will be cleared.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the CPU protect related counters.

Example

This example shows how to clear all CPU protect related statistics.

```
Switch# clear cpu-protect counters all
Switch#
```

55-2 cpu-protect safeguard

This command is used to enable or configure the Safeguard Engine. Use the **no** form of this command to disable the Safeguard Engine.

cpu-protect safeguard [threshold *RISING-THRESHOLD FALLING-THRESHOLD***]**

no cpu-protect safeguard [threshold]

Parameters

threshold	(Optional) Specifies to configure the utilization to control when the Safeguard Engine function will activate.
RISING-THRESHOLD	(Optional) Specifies to set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises over the specified percentage, the Safeguard Engine mechanism will initiate. The valid range is from 20 to 100.
FALLING-THRESHOLD	(Optional) Specifies to set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls

	to the specified percentage, the Safeguard Engine mechanism will shut down. The valid range is from 20 to 100.

Default

By default, Safeguard Engine is disabled.

By default, the rising threshold of CPU utilization is 50.

By default, the falling threshold of CPU utilization is 20.

Command Mode

Global Configuration Mode.

Usage Guideline

The Safeguard Engine can help the overall operability of the device by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the CPU utilization of the Switch rises over configured rising threshold, it will enter exhausted mode. In exhausted mode, the Switch limits the bandwidth of receiving ARP and broadcast IP packets.

Example

This example shows how to enable the Safeguard Engine and configure the thresholds, which the rising and falling threshold are 60 and 40 respectively.

```
Switch# configure terminal
Switch(config)# cpu-protect safeguard threshold 60 40
Switch(config)#
```

55-3 cpu-protect sub-interface

This command is used to configure the rate limit for traffic destined for the CPU by sub-interface types. Use the **no** form of this command to revert to the default settings.

cpu-protect sub-interface {manage | protocol | route} pps *RATE*

no cpu-protect sub-interface {manage | protocol | route}

Parameters

RATE	Specifies the threshold value. The unit is packets per second. When set to 0, all packets of the specified sub-interface type will be dropped.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The reasons of packets that are destined to the CPU can be classified into three groups: **manage**, **protocol** and **route**. The sub-interface is a logical interface, which handles the CPU received packets by different groups. Generally speaking, the protocol packets should have higher priority to make sure the functions work normally. The CPU usually is not involved in the routing of packets. In few cases, such as learning new IP address or if the

default route is not specified, some packets will be sent to the CPU for software routing. Use this command to limit the rate of routed packets to avoid the CPU spending too much time for routing packets.

Example

This example shows how to configure the rate limit of packets for the management sub-interface and the threshold is 1000 packets per seconds.

```
Switch# configure terminal
Switch(config)# cpu-protect sub-interface manage pps 1000
Switch(config)#
```

55-4 cpu-protect type

This command is used to configure the rate limit of traffic destined for the CPU by the protocol type. Use the **no** form of this command to revert to the default setting.

cpu-protect type *PROTOCOL-NAME* **pps** *RATE*

no cpu-protect type *PROTOCOL-NAME*

Parameters

PROTOCOL-NAME	Specifies the protocol name to be configured.
RATE	Specifies the threshold value. The unit is packets per second. When set to 0, all packets of the specified protocol are dropped.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

The CPU must handle certain packets, such as routing protocols, Layer 2 protocols, and packets for management. If the traffic destined to the CPU overloads it, the CPU will spend much time processing unnecessary traffic and the routing processes are impacted. To mitigate the impact on the CPU, use this command to control the threshold of individual protocol packets.

The following lists the reference for the supported protocols for the CPU protect type command. According to the purpose of packets destined to CPU, the router creates three virtual sub-interfaces to process the packets:

- **manage** - The packets are destined to any router interface or system network management interface via the interactive access protocol, such as Telnet and SSH.
- **protocol** - The packets are protocol control packets which can be identified by the router.
- **route** - Other packets traversing the router for routing that must be processed by the router's CPU before it can be routed without the CPU's involvement.

The following table lists the supported protocol names for this command:

Protocol Name	Description	Classification (sub-interface)
8021x	Port-based Network Access Control	Protocol
arp	IP Address Resolution Protocol (ARP)	Protocol
dhcp	Dynamic Host Configuration	Protocol
dns	Domain Name Services	Protocol

Icmpv4	IPv4 Internet Control Message Protocol	Protocol
icmpv6-neighbor	IPv6 ICMP Neighbor Discover Protocol (NS/NA/RS/RA)	Protocol
icmpv6-other	IPv6 ICMP except NDP NS/NA/RS/RA	Protocol
igmp	Internet Group Management Protocol	Protocol
lacp	Link Aggregation Control Protocol	Protocol
snmp	Simple Network Management Protocol	Manage
ssh	Secured shell	Manage
stp	Spanning Tree Protocol (802.1D)	Protocol
telnet	Telnet	Manage
tftp	Trivial File Transfer Protocol	Manage
web	HTTP and HTTPS	Manage

Example

This example shows how to configure the threshold of ARP protocol packets as 100 packets per second.

```
Switch#configure terminal
Switch(config)# cpu-protect type arp pps 100
Switch(config)#
```

55-5 show cpu-protect safeguard

This command is used to display the settings and status of the Safeguard Engine.

show cpu-protect safeguard

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the settings and status of the Safeguard Engine.

Example

This example shows how to display the settings and current status of the Safeguard Engine.

```
Switch#show cpu-protect safeguard

Safeguard Engine State: Disabled
Safeguard Engine Status: Normal
Utilization Thresholds:
 Rising   :30%
 Falling  :20%

Switch#
```

Display Parameters

Safeguard Engine Status	Displays the current mode that CPU utilization stays. The possible displayed strings are: • **Exhausted** - If the CPU utilization is higher than the configured rising threshold, it will enter Exhausted Mode and Safeguard Engine will take actions. The Safeguard Engine mechanism ceases till the utilization is lower than the falling threshold. • **Normal** - The Safeguard Engine is not triggered to take actions.

55-6 show cpu-protect sub-interface

This command is used to display the rate limit and statistics by sub-interface.

show cpu-protect sub-interface {manage | protocol | route}

Parameters

manage	Specifies the manager sub-interface to be displayed.
protocol	Specifies the protocol sub-interface to be displayed.
route	Specifies the route sub-interface to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the configured rate limit and drop count of the safeguard engine of a specific group. These counters are counted by the software.

Example

This example shows how to display the configured rate limit and drop count of the safeguard engine of a specific group..

```
Switch#show cpu-protect sub-interface manage

Sub-Interface: manage
Rate Limit: N/A

Switch#
```

55-7 show cpu-protect type

This command is used to display the rate limit and statistics of CPU protection.

show cpu-protect type *PROTOCOL-NAME*

Parameters

PROTOCOL-NAME	Specifies the configured rate limit and statistics of the specified protocol to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the rate limit and statistics of the safeguard engine.

Example

This example shows how to display the rate limit and statistics of the safeguard engine.

```
Switch#show cpu-protect type arp

Type: arp
Rate Limit: N/A

Switch#
```

55-8 snmp-server enable traps safeguard-engine

This command is used to enable the sending of SNMP notifications for the Safeguard Engine. Use the **no** form of this command to disable the sending of SNMP notifications for the Safeguard Engine.

snmp-server enable traps safeguard-engine

no snmp-server enable traps safeguard-engine

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for the Safeguard Engine.

Example

This example shows how to enable the sending of SNMP notifications for the Safeguard Engine.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps safeguard-engine
Switch(config)#
```

56. Secure Shell (SSH) Commands

56-1 crypto key generate

This command is used to generate the RSA or DSA key pair.

crypto key generate {rsa [modulus *MODULUS-SIZE***] | dsa}**

Parameters

rsa	Specifies to generate the RSA key pair.
modulus *MODULUS-SIZE*	(Optional) Specifies the number of bits in the modulus. For RSA, the valid values are 360, 512, 768, 1024, and 2048.If not specified, a message will be promoted to the user to specify the value.
dsa	Specifies to generate the DSA key pair. The DSA key size is fixed as 1024 bit.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to generate the RSA or DSA key pair.

Example

This example shows how to create an RSA key.

```
Switch#crypto key generate rsa

The RSA key pairs already existed.
Do you really want to replace them? (y/n) [n]y
Choose the size of the key modulus in the range of 360 to 2048.The process may take
a few minutes.
Number of bits in the modulus [768]: 768
Generating RSA key...Done

Switch#
```

56-2 crypto key zeroize

This command is used to delete the RSA or DSA key pair.

crypto key zeroize {rsa | dsa}

Parameters

rsa	Specifies to delete the RSA key pair.
dsa	Specifies to delete the DSA key pair.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to delete the public key pair of the SSH Server. If both RSA and DSA key pairs are deleted, the SSH server will not be in service.

Example

This example shows how to delete the RSA key.

```
Switch#crypto key zeroize rsa

Do you really want to remove the key? (y/n)[n]: y

Switch#
```

56-3 ip ssh timeout

This command is used to configure the SSH control parameters on the Switch. Use the **no** form of this command to revert to the default settings.

ip ssh {timeout *SECONDS* **| authentication-retries** *NUMBER***}**

no ip ssh {timeout | authentication-retries}

Parameters

timeout *SECONDS*	Specifies the time interval that the Switch waits for the SSH client to respond during the SSH negotiation phase The range is from 30 to 600.
authentication-retries *NUMBER*	Specifies the number of authentication retry attempts. The session is closed if all the attempts fail. The range is from 1 to 32.

Default

By default, the timeout value is 120 seconds.

By default, the authentication retries is 3.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the SSH server parameters on the Switch. The authentication retry number specifies the maximum number of retry attempts before the session is closed.

Example

This example shows how to configure the SSH timeout value to 160 seconds.

```
Switch#configure terminal
Switch(config)# ip ssh timeout 160
Switch(config)#
```

This example shows how to configure the SSH authentication retries value to 2 times. The connection fails after 2 retry attempt fails.

```
Switch#configure terminal
Switch(config)# ip ssh authentication-retries 2
Switch(config)#
```

56-4 ip ssh server

This command is used to enable the SSH server function. Use the **no** form of this command to disable the SSH server function.

ip ssh server

no ip ssh server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the SSH server function.

Example

This example shows how to enable the SSH server function.

```
Switch#configure terminal
Switch(config)# ip ssh server
Switch(config)#
```

56-5 ip ssh service-port

This command is used to specify the service port for SSH. Use the **no** form of this command to revert to the default setting.

ip ssh service-port *TCP-PORT*

no ip ssh service-port

Parameters

TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the SSH protocol is 22.

Default

By default, this value is 22.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the TCP port for SSH server.

Example

This example shows how to change the service port number to 3000.

```
Switch# configure terminal
Switch(config)# ip ssh service-port 3000
Switch(config)#
```

56-6 show crypto key mypubkey

This command is used to display the RSA or DSA public key pairs.

show crypto key mypubkey {rsa | dsa}

Parameters

rsa	Specifies to display information regarding the RSA public key.
dsa	Specifies to display information regarding the DSA public key.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the RSA or DSA public key pairs.

Example

This example shows how to display the information of the RSA public key.

```
Switch# show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Switch#
```

56-7 show ip ssh

This command is used to display the user SSH configuration settings.

show ip ssh

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the SSH configuration settings.

Example

This example shows how to display the SSH configuration settings.

```
Switch# show ip ssh

IP SSH server             : Enabled
IP SSH service port       : 22
SSH server mode           : V2
Authentication timeout    : 120 secs
Authentication retries    : 3 times

Switch#
```

56-8 show ssh

This command is used to display the status of SSH server connections.

show ssh

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the status of SSH server connections on the Switch.

Example

This example shows how to display the status of SSH server connections.

```
Switch# show ssh

SID Ver. Cipher                       Userid           Client IP Address
--- --- ---------------------------- ---------------- -------------------------
0   V2  3des-cbc/hmac-sha1-96       zhang3           192.168.0.100
1   V2  3des-cbc/hmac-sha1          lee4567890123456 2000::243

Total Entries: 2

Switch#
```

Display Parameters

SID	A unique number that identifies the SSH session.
Ver	Indicates the SSH version of this session.
Cipher	The cryptographic / Hashed Message Authentication Code (HMAC) algorithm that the SSH client is using.
Userid	The login username of the session.
Client IP Address	The client IP address for this established SSH session.

56-9 ssh user authentication-method

This command is used to configure the SSH authentication method for a user account. Use the **no** form of this command to revert to the default settings.

ssh user *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

no ssh user NAME authentication-method

Parameters

NAME	Specifies the username to configure the authentication type. The user must be an existing local account. The length of the username is limited to a maximum of 32 characters.
password	Specifies to use the password authentication method for this user account. This is the default authentication method.
publickey *URL*	Specifies to use the public key authentication method for this user account. Enter the URL of a local file to be used as the public key of this user.
hostbased *URL*	Specifies to use the host-based authentication method for this user account. Enter the URL of a local file to be used as client's host key.
host-name *HOSTNAME*	Specifies the allowed host name for host-based authentication. During authentication phase, the client's hostname will be checked. The range is from 1 to 255.
IP-ADDRESS	(Optional) Specifies whether to additionally check the IP address of the client for host-based authentication. If not specified, only the host name will be checked.
IPV6-ADDRESS	(Optional) Specifies whether to additionally check the IPv6 address of the client for host-based authentication. If not specified, only the host name will be checked.

Default

The default authentication method for a user is **password**.

Command Mode

Global Configuration Mode.

Usage Guideline

The administrator can use this command to specify authentication method for a user. The user name must be a user created by the username command. By default, the authentication method is password. The system will prompt the user to input the password.

To authenticate a user via SSH public key authentication, copy the user's public key file to file system. When the user tries to login to the Switch via an SSH client (using the SSH public key method), the SSH client will automatically transmit the public key and signature with the private key to the Switch. If both the public key and signature are correct, the user is authenticated and login into the Switch is allowed.

- To authenticate a user via SSH public key authentication via SSH public key or the host-based method, the user's public key file or client's host key file must be specified. Both key files have the same format. A key file can contain multiple keys and each key is defined by one line. The maximum length of one line is 8 Kb.
- Each key consists of the following space-separated fields: *keytype*, *base64-encoded key*, and *comment*. The *keytype* and *base64-encoded key* fields are mandatory and the *comment* field is optional. The *keytype* field can be either be *ssh-dss* or *ssh-rsa*.

Example

This example shows how to configure the authentication method to public key for user user1.

```
Switch# configure terminal
Switch(config)# ssh user tom authentication-method publickey c:/user1.pub
Switch(config)#
```

57. Simple Network Management Protocol (SNMP) Commands

57-1 show snmp trap link-status

This command is used to display the per interface link status trap state.

show snmp trap link-status [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display per interface link up/down trap state. If no parameter is specified, all interfaces will be displayed.

Example

This example shows how to display the link up/down trap state on ports 1 to 9.

```
Switch# show snmp trap link-status interface eth1/0/1-9

Interface       Trap state
-------       -------------
 eth1/0/1        Enabled
 eth1/0/2        Enabled
 eth1/0/3        Disabled
 eth1/0/4        Enabled
 eth1/0/5        Enabled
 eth1/0/6        Disabled
 eth1/0/7        Enabled
 eth1/0/8        Enabled
 eth1/0/9        Enabled

Switch#
```

57-2 show snmp-server

This command is used to display the SNMP server's global state settings and trap related settings.

show snmp-server [traps]

Parameters

traps	(Optional) Specifies to display trap related settings.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use the **show snmp-server** command to display the SNMP server global state settings.

Use the **show snmp-server traps** command to display trap related settings.

Example

This example shows how to display the SNMP server configuration.

```
Switch# show snmp-server

SNMP Server  : Enabled
Name         : SiteA-Switch
Location     : HQ 15F
Contact      : MIS Department II
SNMP UDP Port: 50000
SNMP Response Broadcast Request: Enabled

Switch#
```

This example shows how to display trap related settings.

```
Switch# show snmp-server traps

Global Trap State : Enabled
Individual Trap State:
  Authentication           : Enabled
  linkup                   : Enabled
  linkdown                 : Enabled
  coldstart                : Enabled
  warmstart                : Disabled

Switch#
```

57-3 show snmp-server trap-sending

This command is used to display the per port SNMP trap sending state.

show snmp-server trap-sending [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the per port trap sending state. If no parameter is specified, all interfaces will be displayed.

Example

This example shows how to display the trap sending state on ports 1 to 9.

```
Switch# show snmp-server trap-sending interface eth1/0/1-9

       Port                          Trap Sending
-----------------                   ---------------
 eth1/0/1                              Enabled
 eth1/0/2                              Enabled
 eth1/0/3                              Disabled
 eth1/0/4                              Enabled
 eth1/0/5                              Enabled
 eth1/0/6                              Disabled
 eth1/0/7                              Enabled
 eth1/0/8                              Enabled
 eth1/0/9                              Enabled

Switch#
```

57-4 snmp-server

This command is used to enable the SNMP agent. Use the **no** form of this command to disable the SNMP agent.

snmp-server

no snmp-server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The SNMP manager manages a SNMP agent by sending SNMP requests to agents and receiving SNMP responses and notifications from agents. The SNMP server on the agent must be enabled before the agent can be managed.

Example

This example shows how to enable the SNMP server.

```
Switch# configure terminal
Switch(config)# snmp-server
Switch(config)#
```

57-5 snmp-server contact

This command is used to configure the system contact information for the device. Use the **no** form of this command to remove the setting.

snmp-server contact *TEXT*

no snmp-server contact

Parameters

TEXT	Specifies a string for describing the system contact information. The maximum length is 255 characters The syntax is a general string that allows spaces.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the system contact information for management of the device.

Example

This example shows how to configure the system contact information with the string MIS Department II.

```
Switch# configure terminal
Switch(config)# snmp-server contact MIS Department II
Switch(config)#
```

57-6 snmp-server enable traps

This command is used to enable the sending of trap packets globally. Use the **no** form of this command to disable the sending of trap packets.

snmp-server enable traps

no snmp-server enable traps

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the device to send the SNMP notification traps globally.

Example

This example shows how to enable the SNMP traps global sending state.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)#
```

57-7 snmp-server enable traps snmp

This command is used to enable the sending of all or specific SNMP notifications. Use the **no** form of this command to disable the sending of all or specific SNMP notifications.

snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

Parameters

authentication	(Optional) Specifies to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
linkup	(Optional) Specifies to control the sending of SNMP linkUp notifications. A linkup (3) trap is generated when the device recognizes that one of the communication links has come up.
linkdown	(Optional) Specifies to control the sending of SNMP linkDown notifications. A linkDown (2) trap is generated when the device recognizes a failure in one of the communication links.
coldstart	(Optional) Specifies to control the sending of SNMP coldStart notifications.

warmstart	(Optional) Specifies to control the sending of SNMP warmStart notifications.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of SNMP standard notification traps. To enable the sending of notification traps, the global setting must be enabled too.

Example

This example shows how to enable the switch to send all SNMP traps to the host 10.9.18.100 using the community string defined as public.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps snmp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

This example shows how to enable the SNMP authentication traps.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps snmp authentication
Switch(config)#
```

57-8 snmp-server location

This command is used to configure the system's location information. Use the **no** form of this command to remove the setting.

snmp-server location *TEXT*

no snmp-server location

Parameters

TEXT	Specifies the string that describes the system location information. The maximum length is 255 characters. The syntax is a general string that allows spaces.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the system's location information on the Switch.

Example

This example shows how to configure the system's location information with the string "HQ 15F".

```
Switch# configure terminal
Switch(config)# snmp-server location HQ 15F
Switch(config)#
```

57-9 snmp-server name

This command is used to configure the system's name information. Use the **no** form of this command to remove the setting.

snmp-server name *NAME*

no snmp-server name

Parameters

NAME	Specifies the string that describes the SNMP server name information. The maximum length is 255 characters. It is recommended not to configure the name longer than 10 characters.

Default

By default, this name is "Switch".

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the system's name information on the Switch.

Example

This example shows how to configure the system's name to "SiteA-switch".

```
Switch# configure terminal
Switch(config)#snmp-server name SiteA-switch
SiteA-switch(config)#
```

57-10 snmp-server trap-sending disable

This command is used to disable the sending of notifications for the port. Use the **no** form of this command to enable the sending of notifications for the port.

snmp-server trap-sending disable

no snmp-server trap-sending disable

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to disable or enable the sending of notifications for the port. When disabled, SNMP notification traps generated by the system are not allowed to transmit out of the port. The SNMP traps generated by other system and forwarded to the port is not subject to this restriction.

Example

This example shows how to disable the sending of notifications for port 8.

```
Switch# configure terminal
Switch(config)# interface eth1/0/8
Switch(config-if)# snmp-server trap-sending disable
Switch(config-if)#
```

57-11 snmp-server service-port

This command is used to configure the SNMP UDP port number. Use the **no** form of this command to revert to the default setting.

snmp-server service-port *PORT-NUMBER*

no snmp-server service-port

Parameters

PORT-NUMBER	Specifies the UDP port number. The range is from 1 to 65535. Some numbers may conflict with other protocols.

Default

By default, this number is 161.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the SNNP UDP port number on the Switch. The agent will listen to the SNMP request packets on the configured service UDP port number.

Example

This example shows how to configure the SNMP UDP port number.

```
Switch# configure terminal
Switch(config)# snmp-server service-port 50000
Switch(config)#
```

57-12 snmp-server response broadcast-request

This command is used to enable the server to response to broadcast SNMP GetRequest packets. Use the **no** form of this command to disable the response to broadcast SNMP GetRequest packets.

snmp-server response broadcast-request

no snmp-server response broadcast-request

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the server to response to broadcast SNMP GetRequest packet. NMS tools would send broadcast SNMP GetRequest packets to discover networks device. To support this function, the response to the broadcast get request packet needs to be enabled.

Example

This example shows how to enable the server to respond to the broadcast SNMP get request packet.

```
Switch# configure terminal
Switch(config)# snmp-server response broadcast-request
Switch(config)#
```

57-13 snmp trap link-status

This command is used to enable the notification of link-up and link-down events that occurred on the interface. Use the **no** form of this command to disable the notification.

snmp trap link-status

no snmp trap link-status

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of link-up and link-down traps on an interface.

Example

This example shows how to disable the generation of link-up and link-down traps on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no snmp trap link-status
Switch(config-if)#
```

57-14 show snmp

This command is used to display the SNMP settings.

show snmp {community | host | view | group | engineID}

Parameters

community	Specifies to display SNMP community information.
host	Specifies to display SNMP trap recipient information.
view	Specifies to display SNMP view information.
group	Specifies to display SNMP group information.
engineID	Specifies to display SNMP local engine ID information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the SNMP information. When displaying SNMP community strings, the SNMPv1 or SNMPv2c user created will not be displayed.

Example

This example shows how to display SNMP community information.

```
Switch#show snmp community

Community : public
 Access : read-only
 View : CommunityView

Community : private
 Access : read-write
 View : CommunityView

Total Entries: 2

Switch#
```

This example shows how to display the SNMP server host setting.

```
Switch# show snmp host

Host IP Address  : 10.20.30.40
SNMP Version     : V1
Community Name   : public
UDP Port         : 50001

Host IP Address  : 10.10.10.1
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user1
UDP Port         : 50001

Host IPv6 Address: 1:12:123::100
SNMP Version     : V3 noauthnopriv
SNMPv3 User Name : user2
UDP Port         : 162

Total Entries: 3

Switch#
```

This example shows how to display the MIB view setting.

```
Switch#show snmp view

View Name                Subtree              View Type
------------------------------------------------------------------
restricted               1.3.6.1.2.1.1                included
restricted               1.3.6.1.2.1.11               included
restricted               1.3.6.1.6.3.10.2.1           included
restricted               1.3.6.1.6.3.11.2.1           included
restricted               1.3.6.1.6.3.15.1.1           included
CommunityView            1                            included
CommunityView            1.3.6.1.6.3                  excluded
CommunityView            1.3.6.1.6.3.1                included

Total Entries: 8

Switch#
```

This example shows how to display the SNMP group setting.

```
Switch# show snmp group

GroupName: public                           SecurityModel: v1
  ReadView     : CommunityView              WriteView    :
  NotifyView   : CommunityView
IP access control list:

GroupName: public                           SecurityModel: v2c
  ReadView     : CommunityView              WriteView    :
  NotifyView   : CommunityView
IP access control list:

GroupName: initial                          SecurityModel: v3/noauth
  ReadView     : restricted                 WriteView    :
  NotifyView   : restricted
IP access control list:

GroupName: private                          SecurityModel: v1
  ReadView     : CommunityView              WriteView    : CommunityView
  NotifyView   : CommunityView
IP access control list:

GroupName: private                          SecurityModel: v2c
  ReadView     : CommunityView              WriteView    : CommunityView
  NotifyView   : CommunityView
IP access control list:

Total Entries: 5

Switch#
```

This example shows how to display the SNMP engine ID.

```
Switch# show snmp engineID

Local SNMP engineID: 800000ab033c1e04a1b9e000

Switch#
```

57-15 show snmp user

This command is used to display information about the configured SNMP user.

show snmp user [*USER-NAME***]**

Parameters

USER-NAME	(Optional) Specifies the name of a specific user to display SNMP information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all configured users will be displayed. The community string created will not displayed by this command.

Example

This example shows how to display SNMP users.

```
Switch# show snmp user authuser

User name: authuser
  Security Model: v2c
  Group Name: VacmGroupName
IP access control list: HB5

User name: authuser
  Security Model: v3 priv
  Group Name: VacmGroupName
  Authentication Protocol: MD5
  Privacy Protocol: DES
  Engine ID: 000000090200000000C025808
IP access control list:

Total Entries: 2

Switch#
```

57-16 snmp-server community

This command is used to configure the community string to access the SNMP. Use the **no** form of this command to remove the community string.

snmp-server community *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***]**

no snmp-server community *COMMUNITY-STRING*

Parameters

COMMUNITY-STRING	Specifies the community with a maximum of 32 alphanumeric characters.
view *VIEW-NAME*	(Optional) Specifies a view name of a previously defined view. It defines the view accessible by the SNMP community.
ro	(Optional) Specifies read-only access.
rw	(Optional) Specifies read-write access.
access *IP-ACL-NAME*	(Optional) Specifies the name of the standard access list to control the user to use this community string to access to the SNMP agent. Specifies the valid user in the source address field of the access list entry.

Default

Community	View Name	Access right
private	CommunityView	Read/Write
public	CommunityView	Read Only

Command Mode

Global Configuration Mode.

Usage Guideline

This command provides an easy way to create a community string for SNMPv1 and SNMPv2c management. When creating a community with the **snmp-server community** command, two SNMP group entries, one for SNMPv1 and one for SNMPv2c, which has the community name as their group names are created. If **view** is not specified, it is permitted to access all objects.

Example

This example shows how create a MIB view “interfacesMibView” and a community string “comaccess” which can do read write access the interfacesMibView view.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

57-17 snmp-server engineID local

This command is used to specify the SNMP engine ID on the local device. Use the **no** form of this command to revert to the default setting.

snmp-server engineID local *ENGINEID-STRING*

no snmp-server engineID local

Parameters

ENGINEID-STRING	Specifies the engine ID string of a maximum of 24 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

An SNMP engine ID is not displayed or stored in the running configuration. The SNMP engine ID is a unique string to identify the device. A string is generated by default. If you configure a string less than 24 characters, it will be filled with trailing zeros up to 24 characters.

Example

This example shows how to configure the SNMP engine ID to 332200000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 332200000000000000000000
Switch(config)#
```

57-18 snmp-server group

This command is used to configure an SNMP group. Use the **no** form of this command to remove a SNMP group or remove a group from using a specific security model.

snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *READ-VIEW***] [write** *WRITE-VIEW***] [notify** *NOTIFY-VIEW***] [access** *IP-ACL-NAME***]**

no snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}}**

Parameters

GROUP-NAME	Specifies the group name of a maximum of 32 characters. The syntax is general string that does not allow space.
v1	Specifies that the group user can use the SNMPv1 security model.
v2c	Specifies that the group user can use the SNMPv2c security model.
v3	Specifies that the group user can use the SNMPv3 security model.
auth	Specifies to authenticate the packet but not encrypt it.
noauth	Specifies not to authenticate and not to encrypt the packet.
priv	Specifies to authenticate and encrypt the packet.
read *READ-VIEW*	(Optional) Specifies a read-view that the group user can access.
write *WRITE-VIEW*	(Optional) Specifies a write-view that the group user can access.
notify *NOTIFY-VIEW*	(Optional) Specifies a write-view that the group user can access. The notify view describes the object that can be reported its status via trap packets to the group user.
access *IP-ACL-NAME*	(Optional) Specifies the standard IP access control list (ACL) to associate with the group.

Default

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View Name
Initial	SNMPv3	noauth	Restricted	None	Restricted
Public	SNMPv1	None	CommunityView	None	CommunityView
Public	SNMPv2c	None	CommunityView	None	CommunityView
Private	SNMPv1	None	CommunityView	CommunityView	CommunityView
Private	SNMPv2c	None	CommunityView	CommunityView	CommunityView

By default, no ACL is associated with any SNMP group.

Command Mode

Global Configuration Mode.

Usage Guideline

An SNMP group defines a user group by specifying the allowed security model, the read-view, the write-view, and the notification view. The security model defines that the group user is allowed to use the specified version of SNMP to access the SNMP agent,

The same group name can be created with security models SNMPv1, SNMPv2c, and SNMPv3 at the same time. For SNMPv3, it can be created for SNMPv3 auth and SNMPv3 priv at the same time.

To update the view profile for a group for a specific security model, delete and create the group with the new view profile.

The read-view defines the MIB objects that the group user is allowed to read. If read-view is not specified, then Internet OID space 1.3.6.1 can be read.

The write-view defines the MIB objects that the group user is allowed to write. If write-view is not specified, then no MIB objects can be written.

The notification view defines the MIB objects that the system can report its status in the notification packets to the trap managers that are identified by the specified group user (act as community string). If notify-view is not specified, then no MIB objects can be reported.

Example

This example shows how to create the SNMP server group “guestgroup” for SNMPv3 access and SNMPv2c.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)# snmp-server group guestgroup v2c read CommunityView write CommunityView
Switch(config)#
```

57-19 snmp-server host

This command is used to specify the recipient of the SNMP notification. Use the **no** form of this command to remove the recipient.

snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [version {1 | 2c | 3 {auth | noauth | priv}}]** *COMMUNITY-STRING* **[port** *PORT-NUMBER***]**

no snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [***COMMUNITY-STRING***]**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the SNMP notification host.
IPV6-ADDRESS	Specifies the IPv6 address of the SNMP notification host.
version	(Optional) Specifies the version of the SNMP used to send the traps. If not specified, the default is SNMPv1. • **1** - SNMPv1. • **2c** - SNMPv2c. • **3** - SNMPv3.
auth	(Optional) Specifies to authenticate the packet but not to encrypt it.
noauth	(Optional) Specifies not to authenticate and to encrypt the packet.
priv	(Optional) Specifies to both authenticate and to encrypt the packet.
COMMUNITY-STRING	Specifies the community string to be sent with the notification packet. If the version is 3, the community string is used as the username as defined in the snmp-sever user command.
PORT-NUMBER	(Optional) Specifies the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.

Default

By default, the version used is 1.

Command Mode

Global Configuration Mode.

Usage Guideline

SNMP notifications are sent as trap packets. The user should create at least one recipient of a SNMP notification by using the **snmp-server host** command in order for the Switch to send the SNMP notifications. Specify the version of the notification packet for the created user. For SNMPv1 and SNMPv2c, the notification will be sent in the trap protocol data unit (PDU). For SNMPv3, the notification will be sent in the SNMPv2-TRAP-PDU with the SNMPv3 header.

When specifying to send the trap packets in SNMPv1 or SNMPv2c to a specific host, the specified community string acts as the community string in the trap packets.

When specifying to send the trap packets in SNMPv3 to a specific host, whether to do authentication and encryption in the sending of the packet should be specified. The specified community string acts as the username in the SNMPv3 packet. The user must be created first using the **snmp-server user** command or **snmp-server user v3** command.

In the sending of the trap packet, the system will check the notification view associated with the specified user (or community name). If the binding variables to be sent with the trap packet are not in the notification view, the notification will not be sent to this host.

Example

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with community string “comaccess”.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 3 authentication security level and with the username “useraccess”.

```
Switch# configure terminal
Switch(config)# snmp-server group groupaccess v3 auth read CommunityView write CommunityView
Switch(config)# snmp-server user useraccess groupaccess v3 auth md5 12345678
Switch(config)# snmp-server host 163.10.50.126 version 3 auth useraccess
Switch(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with the community string “comaccess”. The UDP port number is configured to 50001.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess port 50001
Switch(config)#
```

57-20 snmp-server user

This command is used to create an SNMP user. Use the **no** form of this command to remove an SNMP user.

snmp-server user *USER-NAME GROUP-NAME* **[encrypted] [auth {md5 | sha}** *AUTH-PASSWORD* **[priv** *PRIV-PASSWORD*]] **[access** *IP-ACL-NAME*]

no snmp-server user *USER-NAME GROUP-NAME*

Parameters

USER-NAME	Specifies a username of a maximum of 32 characters. The syntax is general string that does not allow spaces.
GROUP-NAME	Specifies the name of the group to which the user belongs. The syntax is general string that does not allow spaces.
encrypted	(Optional) Specifies that the following password is in encrypted format.
auth	(Optional) Specifies the authentication level.
md5	(Optional) Specifies to use HMAC-MD5-96 authentication.
sha	(Optional) Specifies to use HMAC-SHA-96 authentication.
AUTH-PASSWORD	(Optional) Specifies the authentication password in the plain-text form. This password is 8 to 16 octets for MD5 and 8 to 20 octets for SHA. If the **encrypted** parameter is specified, the length is 32 for MD5 and 40 for SHA. The format is a hexadecimal value.
priv	(Optional) Specifies the type of encryption.
PRIV-PASSWORD	(Optional) Specifies the private password in the plain-text form. This password can be up to 16 characters. If the **encrypted** parameter is specified, the length is fixed to 32 octets.
access *IP-ACL-NAME*	(Optional) Specifies the standard IP access control list (ACL) to associate with the user.

Default

By default, there is one user.

User Name: initial.

Group Name: initial.

Command Mode

Global Configuration Mode.

Usage Guideline

To create a SNMP user, specify the security model that the user uses and the group that the user is created for. To create an SNMPv3 user, the password used for authentication and encryption needs to be specified.

An SNMP user is unable to be deleted if it has been associated with a SNMP server host.

Example

This example shows how to configure the plain-text password for the user “user1” in the SNMPv3 group public.

```
Switch#configure terminal
Switch(config)# snmp-server user user1 public v3 auth md5 authpassword priv privpassword
Switch(config)#
```

This example shows how to use the MD5 digest string instead of the plain text password.

```
Switch#configure terminal
Switch(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

57-21 snmp-server view

This command is used to create or modify a view entry. Use the **no** form of this command to remove a specified SNMP view entry.

snmp-server view *VIEW-NAME OID-TREE* **{included | excluded}**

no snmp-server view *VIEW-NAME*

Parameters

VIEW-NAME	Specifies the name of the view entry. The valid length is 1 to 32 characters. The syntax is general string that does not allow spaces.
OID-TREE	Specifies the object identifier of the ASN.1 sub-tree to be included or excluded from the view. To identify the sub-tree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system. Use the asterisk (*) wildcard in a single sub-identifier to specify a sub-tree family.
included	Specifies the sub-tree to be included in the SNMP view.
excluded	Specifies the sub-tree to be excluded from the SNMP view.

Default

VIEW-NAME	OID-TREE	View Type
Restricted	1.3.6.1.2.1.1	Included
Restricted	1.3.6.1.2.1.11	Included
Restricted	1.3.6.1.6.3.10.2.1	Included
Restricted	1.3.6.1.6.3.11.2.1	Included
Restricted	1.3.6.1.6.3.15.1.1	Included
CommunityView	1	Included

CommunityView	1.3.6.1.6.3	Excluded
CommunityView	1.3.6.1.6.3.1	Included

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create a view of MIB objects.

Example

This example shows how to create a MIB view called “interfacesMibView” and define an SNMP group “guestgroup” with “InterfaceMIBView” as the read view.

```
Switch#configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

58. Spanning Tree Protocol (STP) Commands

58-1 clear spanning-tree detected-protocols

This command is used to restart the protocol migration.

clear spanning-tree detected-protocols {all | interface *INTERFACE-ID***}**

Parameters

all	Specifies to trigger the detection action for all ports.
interface *INTERFACE-ID*	Specifies the port interface that will be triggered the detecting action.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to force the port protocol migrating state machine to the *SEND_RSTP* state. This action can be used to test whether all legacy bridges on a given LAN have been removed. If there is no STP Bridge on the LAN, the port will be operated in the configured mode, either in the RSTP or MSTP mode. Otherwise, the port will be operated in the STP mode.

Example

This example shows how to trigger the protocol migration event for all ports.

```
Switch# clear spanning-tree detected-protocols all

Clear spanning-tree detected-protocols? (y/n) [n] y

Switch#
```

58-2 show spanning-tree

This command is used to display the information of spanning tree protocol operation. This command is only for STP and RSTP.

show spanning-tree [interface [_INTERFACE-ID_ **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the Spanning Tree configuration for the single spanning tree when in the RSTP or STP-compatible mode.

Example

This example shows how to display the spanning tree information when STP is enabled.

```
Switch#show spanning-tree

 Spanning Tree: Enabled
 Protocol Mode: RSTP
 Tx-hold-count: 6
 Root ID Priority: 32768
         Address: 3C-1E-04-A1-B9-E0
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge  ID Priority: 32768 (priority 32768  sys-id-ext 0)
         Address: 3C-1E-04-A1-B9-E0
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec,
 Topology Changes Count: 0

                                            Priority Link
 Interface      Role       State      Cost     .Port#   Type   Edge
 ---------      ----       -----      ----     -------  -----  ----
 eth1/0/3       designated forwarding 20000    128.3    p2p    non-edge
 eth1/0/5       backup     blocking   200000   128.5    p2p    non-edge
 eth1/0/6       backup     blocking   200000   128.6    shared non-edge
 eth1/0/7       root       forwarding 2000     128.7    P2p    non-edge

Switch#
```

58-3 show spanning-tree configuration interface

This command is used to display the information about STP interface related configuration.

show spanning-tree configuration interface [*INTERFACE-ID* **[, | -]]**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display Spanning Tree interface level configuration. The command can be used for all STP versions.

Example

This example shows how to display spanning tree configuration information of port 1.

```
Switch# show spanning-tree configuration interface eth1/0/1

eth1/0/1
 Spanning tree state : Enabled
 Port path cost: 0
 Port priority: 128
 Port Identifier:  128.1
 Link type: auto
 Port fast: auto
 Guard root: Disabled
 TCN filter : Disabled
 Bpdu forward: Disabled

Switch#
```

58-4 snmp-server enable traps stp

This command is used to enable the sending of SNMP notifications for STP. Use the **no** form of this command to disable the sending of notifications for STP.

snmp-server enable traps stp [new-root] [topology-chg]

no snmp-server enable traps stp [new-root] [topology-chg]

Parameters

new-root	(Optional) Specifies the sending of STP new root notification.
topology-chg	(Optional) Specifies the sending of STP topology change notification.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of notification traps for STP. If no parameter is specified, both STP notification types are enabled or disabled.

Example

This example shows how to enable the sending of the all traps for STP to the host 10.9.18.100 using the community string defined as public.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps stp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

58-5 spanning-tree global state

This command is used to enable the global state of STP. Use the **no** form of this command to disable the state.

spanning-tree global state {enable | disable}

no spanning-tree global state

Parameters

enable	Specifies to enable the STP's global state.
disable	Specifies to disable the STP's global state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the global state of STP.

Example

This example shows how to enable the STP function.

```
Switch# configure terminal
Switch(config)# spanning-tree global state enable
Switch(config)#
```

58-6 spanning-tree (timers)

This command is used to configure the Spanning Tree timer value. Use the **no** form of this command to revert to the default settings.

spanning-tree {hello-time *SECONDS* **| forward-time** *SECONDS* **| max-age** *SECONDS***}**

no spanning-tree {hello-time | forward-time | max-age}

Parameters

hello-time *SECONDS*	Specifies the interval that a designated port will wait between the periodic transmissions of each configuration message. The range is from 1 to 2 seconds.
forward-time *SECONDS*	Specifies the forward delay time used by STP to transition from the listening to the learning states and learning to forwarding states. The range is from 4 to 30 seconds.
max-age *SECONDS*	Specifies the maximum message age of BPDU. The range is from 6 to 40 seconds.

Default

The default value of the **hello-time** is 2 seconds.

The default value of the **forward-time** is 15 seconds.

The default value of the **max-age** is 20 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the Spanning Tree timer value.

Example

This example shows how to configure the STP timers.

```
Switch# configure terminal
Switch(config)# spanning-tree hello-time 1
Switch(config)# spanning-tree forward-time 16
Switch(config)# spanning-tree max-age 21
Switch(config)#
```

58-7 spanning-tree state

This command is used to enable or disable the STP operation. Use the **no** form of this command to revert to the default setting.

spanning-tree state {enable | disable}

no spanning-tree state

Parameters

enable	Specifies to enable STP for the configured interface.
disable	Specifies to disable STP for the configured interface.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

When a port is spanning tree enabled, the spanning tree protocol engine will either send or process the spanning tree BPDU received by the port. The command should be used with caution to prevent bridging loops. The command does not take effect if the Layer 2 protocol tunnel is enabled for STP.

Example

This example shows how to enable spanning tree on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree state enable
Switch(config-if)#
```

58-8 spanning-tree cost

This command is used to configure the value of the port path-cost on the specified port. Use the **no** form of this command to revert to the auto-computed path cost.

spanning-tree cost *COST*

no spanning-tree cost

Parameters

COST	Specifies the path cost for the port. The range is from 1 to 200000000.

Default

The default path cost is computed from the interface's bandwidth setting.

Command Mode

Interface Configuration Mode.

Usage Guideline

In the RSTP or STP-compatible mode, the administrative path cost is used by the single spanning-tree to accumulate the path cost to reach the Root. In the MSTP mode, the administrative path cost is used by the CIST regional root to accumulate the path cost to reach the CIST root.

Example

This example shows how to configure the port cost to 20000 on port 7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree cost 20000
Switch(config-if)#
```

58-9 spanning-tree guard root

This command is used to enable the root guard mode. Use the **no** form of this command to revert to the default setting.

spanning-tree guard root

no spanning-tree guard root

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

BPDU guard prevents a port from becoming a root port. This feature is useful for the service provider to prevent external bridges to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator.

When a port is guarded from becoming a root port, the port will only play the role as a designated port. If the port receives the configuration BPDU with a higher priority, the port will change to the alternate port, which is in the blocking state. The received superior factor will not participate in the STP computation. The port will listen for BPDUs on the link. If the port times out the received superior BPDU, it will change to the designated port role.

When a port changes to the alternate port state, due to the root guard, a system message will be generated. This configuration will take effect for all the spanning-tree versions.

Example

This example shows how to configure to prevent port 1 from being a root port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

58-10 spanning-tree link-type

This command is used to configure a link-type for a port. Use the **no** form of this command to revert to the default setting.

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

Parameters

point-to-point	Specifies that the port's link type is point-to-point.
shared	Specifies that the port's link type is a shared media connection.

Default

The link type is automatically derived from the duplex setting unless explicitly configuring the link type.

Command Mode

Interface Configuration Mode.

Usage Guideline

A full-duplex port is considered to have a point-to-point connection; on the opposite, a half-duplex port is considered to have a shared connection .The port can't transit into forwarding state rapidly by setting link type to shared-media. Hence, auto-determined of link-type by the STP module is recommended.

This configuration will take effect for all the spanning-tree modes.

Example

This example shows how to configure the link type to point-to-point on port 7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)#
```

58-11 spanning-tree mode

This command is used to configure the STP mode. Use the **no** form of this command to revert to the default setting.

spanning-tree mode {mstp | rstp |stp}

no spanning-tree mode

Parameters

mstp	Specifies the Multiple Spanning Tree Protocol (MSTP).
rstp	Specifies the Rapid Spanning Tree Protocol (RSTP).
stp	Specifies the Spanning Tree Protocol (IEEE 802.1D Compatible)

Default

By default, this mode is **rstp**.

Command Mode

Global Configuration Mode.

Usage Guideline

If the mode is configured as STP or RSTP, all currently running MSTP instances will be cancelled automatically. If the newly configured mode is changed from the previous one, the spanning-tree state machine will restart again, therefore all of the stable spanning-tree port states will transit into discarding states.

Example

This example shows how to configure the running version of the STP module to RSTP.

```
Switch# configure terminal
Switch(config)# spanning-tree mode rstp
Switch(config)#
```

58-12 spanning-tree portfast

This command is used to specify the port's fast mode. Use the **no** form of this command to revert to the default setting.

spanning-tree portfast {disable | edge| network}

no spanning-tree portfast

Parameters

disable	Specifies to set the port to the port fast disabled mode.
edge	Specifies to set the port to the port fast edge mode.
network	Specifies to set the port to the port fast network mode.

Default

By default, this option is **edge**.

Command Mode

Interface Configuration Mode.

Usage Guideline

A port can be in one of the following three port fast modes:

- **Edge mode** - The port will directly change to the spanning-tree forwarding state when a link-up occurs without waiting for the forward-time delay. If the interface receives a BPDU later, its operation state changes to the non-port-fast state.
- **Disable mode** - The port will always be in the non-port-fast state. It will always wait for the forward-time delay to change to forwarding state.
- **Network mode** - The port will remain in the non-port-fast state for three seconds. The port will change to the port-fast state if no BPDU is received and changes to the forwarding state. If the port received the BPDU later, it will change to the non-port-fast state

This command should be used with caution. Otherwise, an accidental topology loop and data-packet loop may be generated and disrupt the network operation.

Example

This example shows how to configure port 7 to the port-fast edge mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree portfast edge
Switch(config-if)#
```

58-13 spanning-tree port-priority

This command is used to configure the value of the STP port priority on the specified port. It is only used for RSTP and STP versions. Use the **no** form of this command to revert to the default setting.

spanning-tree port-priority *PRIORITY*

no spanning-tree port-priority

Parameters

PRIORITY	Specifies the port priority. Valid values are from 0 to 240.

Default

By default, this value is 128.

Command Mode

Interface Configuration Mode.

Usage Guideline

The port priority and the port number together form the Port Identifier. It will be used in the computation of the role of the port. This parameter is used only in the RSTP and STP-compatible mode. A smaller number represents a better priority.

Example

This example shows how to configure the port priority to 0 on port 7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

58-14 spanning-tree priority

This command is used to configure the bridge priority. It is only used for RSTP and STP versions. Use the **no** form of this command to restore to the default setting.

spanning-tree priority *PRIORITY*

no spanning-tree priority

Parameters

PRIORITY	Specifies that the bridge priority and bridge MAC address together forms the Spanning-Tree Bridge-ID, which is an important factor in the Spanning-Tree topology. The range is from 0 to 61440.

Default

By default, this value is 32768.

Command Mode

Global Configuration Mode.

Usage Guideline

The bridge priority value is one of the two parameters used to select the Root Bridge. The other parameter is system's MAC address. The bridge's priority value must be divisible by 4096 and a smaller number represents a better priority.

This configuration will take effect on STP version and RSTP mode. In the MSTP mode, use the **spanning-tree mst priority** command to configure the priority for an MSTP instance.

Example

This example shows how to configure the STP bridge priority value to 4096.

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
Switch(config)#
```

58-15 spanning-tree tcnfilter

This command is used to enable Topology Change Notification (TCN) filtering at the specific interface. Use the **no** form of this command to disable TCN filtering.

spanning-tree tcnfilter

no spanning-tree tcnfilter

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Enabling TC filtering on a port is useful for an ISP to prevent the external bridge to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator.

When a port is set to the TCN filter mode, the TC event received by the port will be ignored. This configuration will take effect for all the spanning-tree modes.

Example

This example shows how to configure TCN filtering on port 7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree tcnfilter
Switch(config-if)#
```

58-16 spanning-tree tx-hold-count

This command is used to limit the maximum number of BPDUs that can be sent before pausing for one second. Use the **no** form of this command to revert to the default setting.

spanning-tree tx-hold-count *VALUE*

no spanning-tree tx- hold-count

Parameters

VALUE	Specifies the maximum number of BPDUs that can be sent before pausing for one second. The range is from 1 to 10.

Default

By default, this value is 6.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the number of hold BPDUs to transmit. The transmission of BPDUs on a port is controlled by a counter. The counter is incremented on every BPDU transmission and decremented once a second. The transmissions are paused for one second if the counter reaches the transmit hold count.

Example

This example shows how to configure the transmit hold count value to 5.

```
Switch# configure terminal
Switch(config)# spanning-tree tx-hold-count 5
Switch(config)#
```

58-17 spanning-tree forward-bpdu

This command is used to enable the forwarding of the spanning tree BPDU. Use the **no** form of this command to disable the forwarding of the spanning tree BPDU.

spanning-tree forward-bpdu

no spanning-tree forward-bpdu

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

If enabled, the received STP BPDU will be forwarded to all VLAN member ports in the untagged form. The command does not take effect if the Layer 2 protocol tunnel is enabled for STP.

Example

This example shows how to enable the forwarding of STP BPDUs.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# spanning-tree forward-bpdu
Switch(config-if)#
```

59. Storm Control Commands

59-1 snmp-server enable traps storm-control

This command is used to enable or control the command to enable the sending of SNMP notifications for storm control. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps storm-control [storm-occur] [storm-clear]

no snmp-server enable traps storm-control [storm-occur] [storm-clear]

Parameters

storm-occur	(Optional) Specifies to send a notification when a storm event is detected.
storm-clear	(Optional) Specifies to send a notification when a storm event is cleared.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the sending of notifications for storm control. If no parameter is specified, both **storm-occur** and **storm-clear** parameters are enabled or disabled.

Example

This example shows how to enable the sending of notifications for storm control for both storm occurred and cleared.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps storm-control
Switch(config)#
```

59-2 storm-control

This command is used to configure the device to protect the device from broadcast, multicast, and DA unknown packet storm attacks. Use the **no** form of this command to revert to the default settings.

storm-control {{broadcast | multicast | unicast} level {pps *PPS-RISE* **[***PPS-LOW***] | kbps** *KBPS-RISE* **[***KBPS-LOW***] |** *LEVEL-RISE* **[***LEVEL-LOW***]} | action {shutdown | drop | none}}**

no storm-control {broadcast | multicast | unicast | action}

Parameters

broadcast	Specifies to set the broadcast rate limit.
multicast	Specifies to set the multicast rate limit.
unicast	Specifies to set the unicast rate limit. When the action is configured as the shutdown mode, the unicast refers to both known and unknown unicast packets; that is, if the known and unknown unicast packets hit the specified threshold, the port will be shutdown. Otherwise, unicast refers to unknown unicast packets.

level pps *PPS-RISE* **[***PPS-LOW***]**	Specifies the threshold value in packets count per second. The range is from 0 to 2147483647. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
level kbps *KBPS-RISE* **[***KBPS-LOW***]**	Specifies the threshold value as a rate of bits per second at which traffic is received on the port. The range is from 0 to 2147483647. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.
level *LEVEL-RISE* **[***LEVEL-LOW***]**	Specifies the threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 0 to 100. If the low level is not specified, the default value is 80% of the specified risen level.
action shutdown	Specifies to shut down the port when the value specified for rise threshold is reached.
action drop	Specifies to discards packets that exceed the risen threshold.
action none	Specifies not to filter the storm packets.

Default

By default, the broadcast, multicast, and unicast (DLF) storm controls are disabled.

The default action taken when a storm occurs is to drop storm packets.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use the storm control function to protect the network from the storm of broadcast packets, multicast packets, or unknown DA flooding packets. Enter the **storm-control** command to enable storm control for a specific traffic type on the interface.

There are two ways to recover an error disabled port.

- The user can use the **errdisable recovery cause** command to enable the automatic recovery of ports that were error disabled by storm control.
- The user can manually recover the port by entering the **shutdown** command, followed by the **no shutdown** command for the port.

There is only one meter mode (percentage, kbps or pps) that can take effect on an interface. On an interface, if the later specified meter mode option is different from the previous mode, the previous configured storms will reset to their default states (disabled in this specification).

Due to hardware limitations, when the meter mode is percentage or kbps:

- The action cannot be specified to the shutdown mode.
- There are no traps and logs for the drop and none modes.

This feature is unable to give the precise suppression level of the total bandwidth in percentage (0 to 100) of a specific port interface. The current calculation formula assumes that the packet size is 64 bytes.

Example

This example shows how to enable broadcast storm control on ports 1 and 2. It sets the threshold of port 1 to 500 packets per second with the shutdown action and sets the threshold of port 2 between 60% and 70% with the drop action.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# storm-control broadcast level pps 500
Switch(config-if)# storm-control action shutdown
Switch(config-if)# exit
Switch(config)# interface eth1/0/2
Switch(config-if)# storm-control broadcast level 70 60
Switch(config-if)# storm-control action drop
Switch(config-if)#
```

59-3 storm-control polling

This command is used to configure the polling interval of received packet counts. Use the **no** form of this command to revert to the default settings.

storm-control polling {interval *SECONDS* **| retries {***NUMBER* **| infinite}}**

no storm-control polling {interval | retries}

Parameters

interval *SECONDS*	Specifies the polling interval of received packet counts. This value must be between 5 and 600 seconds.
retries *NUMBE*	Specifies the retry count. If the action is configured to the shutdown mode and a storm continues as long as the interval times retries values set, the port will enter the error disabled state. This value must be between 0 and 360. 0 means that a shutdown mode port will directly enter the error disabled state when a storm is detected. Infinite means that a shutdown mode port will never enter the error disabled state even if a storm was detected.

Default

The default polling interval is 5 seconds.

The default retries count value is 3.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to specify the sample interval of received packet counts.

Example

This example shows how to specify the polling interval as 15 seconds.

```
Switch# configure terminal
Switch(config)# storm-control polling interval 15
Switch(config)#
```

59-4 show storm-control

This command is used to display the current storm control settings.

show storm-control interface *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Parameters

INTERFACE-ID	Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
broadcast	(Optional) Specifies to display the current broadcast storm setting.
multicast	(Optional) Specifies to display the current multicast storm setting.
unicast	(Optional) Specifies to display the current unicast (DLF) storm setting.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no packet type is specified, all types of storm control settings will be displayed.

Example

This example shows how to display the current broadcast storm control settings on ports 1 to 6.

```
Switch#show storm-control interface ethe1/0/1-6 broadcast

 Interface   Action   Threshold            Current      State
 ------------------------------------------------------------------
 eth1/0/1    Drop     500/300 pps          200 pps      Forwarding
 eth1/0/2    Drop     80/64 %              20 %         Forwarding
 eth1/0/3    Drop     80/64 %              80 %         Dropped
 eth1/0/4    Shutdown 600/400 pps          300 pps      Forwarding
 eth1/0/5    None     60000/50000 kbps     2000 kbps    Forwarding
 eth1/0/6    None     -                    -            Inactive

 Total Entries: 6

Switch#
```

This example shows how to display all types of storm control settings on ports 1 to 2.

```
Switch# show storm-control interface eth1/0/1-2

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Trap                      : Disabled
Interface      Storm         Action      Threshold     Current    State
---------------------- ------------------------------------------
eth1/0/1      Broadcast     Drop         80/64 %       50%        Forwarding
eth1/0/1      Multicast     Drop         80/64 %       50%        Forwarding
eth1/0/1      Unicast       Drop         80/64 %       50%        Forwarding
eth1/0/2      Broadcast     Shutdown     500/300 pps   -          Error Disabled
eth1/0/2      Multicast     Shutdown     500/300 pps   -          Error Disabled
eth1/0/2      Unicast       Shutdown     500/300 pps   -          Error Disabled

Total Entries: 6

Switch#
```

Display Parameters

Interface	The interface ID.
Action	The configured action, the possible actions are: Drop, Shutdown, None.
Threshold	The configured threshold.
Current	The actual traffic rate which is currently flowing though the interface. Its unit may be percentage, kbps, PPS based on the configured meter mode. Because hardware can only counts by PPS, this value of this filed may be a rough value for percentage and kbps.
State	The current state of storm control on a given interface for a given traffic type. The possible states are: • **Forwarding** - No storm event has been detected. • **Dropped** - A storm event has occurred and the storm traffic exceeding the threshold is dropped. • **Error Disabled** - The port is disabled due to a storm. • **Link Down** - The port is physically linked down. • **Inactive** - Indicates that storm control is not enabled for the given traffic type.

60. Surveillance VLAN Commands

60-1 surveillance vlan

This command is used to enable the global surveillance VLAN state and configure the surveillance VLAN. Use the **no** form of this command to disable the surveillance VLAN state.

surveillance vlan *VLAN-ID*

no surveillance vlan

Parameters

VLAN-ID	Specifies the ID of the surveillance VLAN. The range is from 2 to 4094.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the global surveillance VLAN function and to specify the surveillance VLAN on the Switch. The Switch has only one Surveillance VLAN. This surveillance VLAN also supports to recognize the surveillance devices, like IP Cameras (IPC) and Network Video Recorders (NVR), using the ONVIF protocol.

Both the **surveillance vlan** command in the Global Configuration Mode and the **surveillance vlan enable** command in the Interface Configuration Mode need to be enabled for a port to start the surveillance VLAN function.

When surveillance VLAN is enabled for a port, the port will automatically be learned as a surveillance VLAN untagged member. Received untagged surveillance packets will be forwarded in surveillance VLAN. Received packets are determined as surveillance packets if the source MAC addresses of packets comply with the OUI addresses configured by the **surveillance vlan mac-address** command.

An auto-surveillance VLAN can also be used to carry video traffic from an IP camera and its related components like Video Management Servers (VMS), VMS clients, and video encoders. These devices can be recognized by an OUI address and the ONVIF protocol. If the IPC is recognized by the ONVIF protocol, the Switch will learn the IPC on a port by snooping Hello/ProbeMatch packets and then insert the port into the surveillance VLAN.

The Switch regards a host as an NVR once it connects to the IPC via HTTP, HTTPS, or RTSP. The Switch will learn the NVR on this port and move it into the surveillance VLAN until the triggered aging mechanism age-out or the LAN cable is removed.

When the host sends an ARP request to an IPC, the Switch still regards the host as an NVR but only temporarily move it into the surveillance VLAN. The host will automatically be moved out of the surveillance VLAN after about 30 seconds if it is not recognized as an NVR anymore.

NOTE: The same PC, or PCs connected to the same LAN port on the Switch, cannot simultaneously manage the Switch and the IP cameras connected to the Switch.

If the IPC is recognized by OUI address, the Switch will determine whether a received packet is a video packet or not by checking its IPC MAC address. If the source MAC addresses of the untagged packets has the same MAC address as the IPC. These packets are determined as video packets and transmitted in surveillance VLANs. If the incoming video packet is tagged, and its VLAN ID is equal to the surveillance VLAN, the priority of the packet will be remarked with video traffic priority.

When the IPC is recognized by its OUI address and ONVIF protocol at the same time, this IPC will be recognized by the ONVIF protocol and take action. If the resource supported ONVIF device is depleted, the IPC will be recognized by OUI address.

The VLAN to be specified as a surveillance VLAN needs to pre-exist to use this command.

If the surveillance VLAN is configured, the surveillance VLAN by the **vlan** command cannot be removed.

Example

This example shows how to enable the surveillance VLAN function and configure VLAN 1001 as a Surveillance VLAN.

```
Switch# configure terminal
Switch(config)# surveillance vlan 1001
Switch(config)#
```

60-2 surveillance vlan aging

This command is used to configure the aging time for aging out the surveillance VLAN dynamic member ports. Use the **no** form of this command to revert to the default setting.

surveillance vlan aging *MINUTES*

no surveillance vlan aging

Parameters

MINUTES	Specifies the aging time of surveillance VLAN. The range is from 1 to 65535 minutes.

Default

By default, this aging time is 720 minutes.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the aging time for aging out the surveillance device and the surveillance VLAN automatically learned member ports.

When the last surveillance device connected to the port stops sending traffic, and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer.

If the surveillance traffic resumes during the aging time, the aging timer will be cancelled.

Example

This example shows how to configure the aging time of surveillance VLAN to 30 minutes.

```
Switch# configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

60-3 surveillance vlan enable

This command is used to enable the surveillance VLAN state of ports. Use the **no** form of this command to disable the surveillance VLAN state of ports.

surveillance vlan enable

no surveillance vlan enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

The command takes effect for access ports or hybrid ports.

Use this command to enable the surveillance VLAN function for ports.

Both the **surveillance vlan** command in Global Configuration Mode and the **surveillance vlan enable** command in Interface Configuration Mode need to be enabled for a port to start the surveillance VLAN function.

When surveillance VLAN is enabled for a port, the port will be automatically learned as surveillance VLAN untagged member, the received untagged surveillance packets will be forwarded to surveillance VLAN. The received packets are determined as surveillance packets if the source MAC addresses of packets comply with the OUI addresses configured by the **surveillance vlan mac-address** command.

Example

This example shows how to enable surveillance VLAN function on port 1.

```
Switch# configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

60-4 surveillance vlan mac-address

This command is used to add the user-defined surveillance device OUI. Use the **no** form of this command to delete the user-defined surveillance device OUI.

surveillance vlan mac-address *MAC-ADDRESS MASK* **[component-type {vms | vms-client | video-encoder | network-storage | other} description** *TEXT***]**

no surveillance vlan mac-address *MAC-ADDRESS MASK*

Parameters

MAC-ADDRESS	Specifies the OUI MAC address.
MASK	Specifies the OUI MAC address matching bitmask.
component-type	(Optional) Specifies surveillance components that could be auto-detected by surveillance VLAN.
vms	(Optional) Specifies the surveillance components type as Video Management Server (VMS).
vms-client	(Optional) Specifies the surveillance components type as VMS client.

video-encoder	(Optional) Specifies the surveillance components type as Video Encoder.
network-storage	(Optional) Specifies the surveillance components type as Network Storage.
other	(Optional) Specifies the surveillance components type as other IP Surveillance Devices.
description *TEXT*	(Optional) Specifies the description for the user-defined OUI with a maximum of 32 characters.

Default

OUI Address	Mask	Component Type	Description
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	D-Link Device	IP Surveillance Device
28-10-7B-20-00-00	FF-FF-FF-F0-00-00	D-Link Device	IP Surveillance Device
B0-C5-54-00-00-00	FF-FF-FF-80-00-00	D-Link Device	IP Surveillance Device
F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	D-Link Device	IP Surveillance Device

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to add user-defined OUI(s) for the surveillance VLAN. The OUI for surveillance VLAN are used to identify the surveillance traffic by the surveillance VLAN function.

If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.

The user-defined OUI cannot be the same as the default OUI.

The default OUI cannot be deleted.

Example

This example shows how to add a user-defined OUI for surveillance devices.

```
Switch# configure terminal
Switch(config)# surveillance vlan mac-address 00-01-02-03-00-00 FF-FF-FF-FF-00-00 component-type vms description user1
Switch(config)#
```

60-5 surveillance vlan onvif-discover-port

This command is used to configure the TCP/UDP port number for RTSP stream snooping. Use the **no** form of this command to revert to the default setting.

surveillance vlan onvif-discover-port *VALUE*

no surveillance vlan onvif-discover-port

Parameters

VALUE	Enter the TCP/UDP port number here. The range is either 554, or from 1025 to 65535.

Default

By default, this value is 554.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the TCP/UDP port number for RTSP stream snooping. ONVIF-capable IPC and ONVIF-capable NVR utilize WS-Discovery to find other devices. Once IPCs are discovered, the Switch can further discover NVRs by snooping RTSP, HTTP, and HTTPS packets between NVRs and IPCs. These packets cannot be snooped if the TCP/UDP port is not equal to the RTSP port number.

Example

This example shows how to configure the TCP/UDP port number to 2000 for RTSP stream snooping.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-discover-port 2000
Switch(config)#
```

60-6 surveillance vlan onvif-ipc state

This command is used to configure the ONVIF recognition IPC state. Use the no form of this command to revert to the default setting.

surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] state {enable | disable}**

no surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] state**

Parameters

IP-ADDRESS	Enter the IP address of the IPC here.
mac-address *MAC-ADDRESS*	(Optional) Enter the MAC address of the IPC that is recognized with ONVIF.
enable	Specifies that the ONVIF recognition IPC state will be enabled.
disable	Specifies that the ONVIF recognition IPC state will be disabled.

Default

By default, this feature is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the ONVIF recognition IPC state with only the IP address of the IPC, or both the IP and MAC address of the IPC. When the ONVIF IPC is recognized, the state can be configured for the specified device. If there is more than one IPC with the same IP address and the MAC addresses of those IPCs are not specified, the state of those IPCs will be affected.

This feature is used to block IPC traffic or not. If the IPC state on the port is disabled, the traffic from the IPC will be blocked.

Example

This example shows how to enable the state of IPC with the IP address 172.18.60.1.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 state enable
Switch(config)#
```

60-7 surveillance vlan onvif-ipc description

This command is used to configure the description of the ONVIF recognized IPC. Use the **no** command to remove the description.

surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description** *TEXT*

no surveillance vlan onvif-ipc *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description**

Parameters

IP-ADDRESS	Enter the IP address of the ONVIF recognized IPC.
mac-address *MAC-ADDRESS*	(Optional) Enter the MAC address of the IPC that is recognized with ONVIF.
TEXT	Enter the description of the ONVIF recognized IPC here. This can be up to 32 characters long.

Default

By default, there is no description defined for an ONVIF recognized IPC.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the description of the ONVIF recognized IPC with only the IP address of the IPC, or both the IP and MAC address of the IPC. If there is more than one IPC with the same IP address and the MAC addresses of those IPCs are not specified, the description of those IPCs will be configured.

Example

This example shows how to define the description of the IPC with an IP address of 172.18.60.1 to 'ipc1'.

```
Switch# configure terminal
Switch(config)# surveillance vlan onvif-ipc 172.18.60.1 description ipc1
Switch(config)#
```

60-8 surveillance vlan onvif-nvr description

This command is used to configure the description of an ONVIF recognized NVR. Use the **no** command to remove this description.

surveillance vlan onvif-nvr *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description** *TEXT*

no surveillance vlan onvif-nvr *IP-ADDRESS* **[mac-address** *MAC-ADDRESS***] description**

Parameters

IP-ADDRESS	Enter the IP address of the ONVIF recognized NVR.
mac-address *MAC-ADDRESS*	(Optional) Enter the MAC address of the NVR that is recognized with ONVIF.
TEXT	Enter the description of the ONVIF recognized NVR here. This can be up to 32 characters long.

Default

By default, there is no description defined for an ONVIF recognized NVR.

Command Mode

Global Configuration Mode.

Usage Guideline

When an ONVIF NVR is recognized, the description for specified device can be configured.

Use this command to configure the description of the ONVIF recognized NVR with only the IP address of the NVR, or both the IP and MAC address of the NVR. If there is more than one NVR with the same IP address and the MAC addresses of those NVRs are not specified, the description of those NVRs will be configured.

Example

This example shows how to define the description of the NVR with an IP address of 172.18.60.2 to 'nvr1'.

```
Switch#configure terminal
Switch(config)# surveillance vlan onvif-nvr 172.18.60.2 description nvr1
Switch(config)#
```

60-9 surveillance vlan qos

This command is used to onfigure the CoS priority for the incoming surveillance VLAN traffic. Use the **no** form of this command to revert to the default settings.

surveillance vlan qos *COS-VALUE*

no surveillance vlan qos

Parameters

COS-VALUE	Specifies the priority of surveillance VLAN. The available value is from 0 to 7.

Default

The default value 5.

Command Mode

Global Configuration Mode.

Usage Guideline

The surveillance packets arriving at the surveillance VLAN enabled port are marked to the COS specified by the command.

The remarking of COS allows the surveillance VLAN traffic to be distinguished from data traffic in quality of service.

Example

This example shows how to configure the priority of the surveillance VLAN to be 7.

```
Switch#configure terminal
Switch(config)# surveillance vlan qos 7
Switch(config)#
```

60-10 show surveillance vlan

This command is used to display the surveillance VLAN configurations.

show surveillance vlan [interface [*INTERFACE-ID* **[, | -]]]**

show surveillance vlan device [interface [*INTERFACE-ID* **[, | -]]]**

Parameters

device	Specifies to display the learned surveillance devices information.
interface *INTERFACE-ID*	(Optional) Specifies to display surveillance VLAN information of ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the surveillance VLAN configurations.

The **show surveillance vlan** command is used to display the surveillance VLAN global configurations.

The **show surveillance vlan interface** command is used to display the surveillance vlan configurations on the interfaces.

The **show surveillance vlan device** command is used to display the surveillance device discovered by its OUI.

Example

This example shows how to display the surveillance VLAN global settings.

```
Switch#show surveillance vlan

 Surveillance VLAN ID  : 100
 Surveillance VLAN CoS : 5
 Aging Time            : 30 minutes
 ONVIF Discover Port   : 554
 Member Ports          :
 Dynamic Member Ports  :

 Surveillance VLAN OUI :

 OUI Address        Mask               Component Type   Description
 -----------------  -----------------  ---------------  --------------
 28-10-7B-00-00-00  FF-FF-FF-E0-00-00  D-Link Device    IP Surveillance Device
 28-10-7B-20-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device
 B0-C5-54-00-00-00  FF-FF-FF-80-00-00  D-Link Device    IP Surveillance Device
 F0-7D-68-00-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device

 Total OUI: 4

Switch#
```

60-11 show surveillance vlan onvif-ipc interface

This command is used to display ONVIF-based IPC information.

show surveillance vlan onvif-ipc interface [*INTERFACE-ID* **[, | -]] {brief | detail}**

Parameters

INTERFACE-ID	(Optional) Specifies the port to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
brief	Specifies to display brief ONVIF-based IP camera information.
detail	Specifies to display detailed ONVIF-based IP camera information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display brief or detailed ONVIF-based IPC information.

Example

This example shows how to display brief ONVIF-based IP camera information.

```
Switch#show surveillance vlan onvif-ipc interface eth1/0/1 brief

Interface    : eth1/0/1
IP Address   : 10.90.90.1
MAC Address  : 00-01-02-03-04-05
Model        : P3384-VE
Manufacturer : D-Link
Traffic      : Enabled
Throughput   : 5 Mbps
Description  : P3384-VE

Total Entries: 1

Switch#
```

This example shows how to display detailed ONVIF-based IP camera information.

```
Switch#show surveillance vlan onvif-ipc interface eth1/0/1 detail

Interface         : eth1/0/1
IP Address        : 10.90.90.1
MAC Address       : 00-01-02-03-04-05
Model             : P3384-VE
Manufacturer      : D-Link
State             : Enabled
Throughput        : 5 Mbps
Description       : P3384-VE
Protocol          : ONVIF
Power Consumption: 1.9W/15W
PoE               : 802.3af
PoE Status        : Enable

Total Entries: 1

Switch#
```

60-12 show surveillance vlan onvif-nvr interface

This command is used to display ONVIF-based NVR and group information.

show surveillance vlan onvif-nvr interface [*INTERFACE-ID* **[, | -]] [ipc-list]**

Parameters

INTERFACE-ID	(Optional) Specifies the port to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
ipc-list	(Optional) Specifies to display NVR group information.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display ONVIF-based NVR and group information. The group ID is the group ID of the IPCs that belong to the NVR group. NVRs and IPCs, managed by it, must have the same group ID.

Example

This example shows how to display ONVIF-based NVR information.

```
Switch# show surveillance vlan onvif-nvr interface eth1/0/1

Interface    : eth1/0/1
IP Address   : 111.111.111.111
MAC Address  : 00-03-02-03-04-08
IPC Number   : 2
Throughput   : 10 Mbps
Group        : Group 1
Description  : D-Link-NVR

Total Entries: 1

Switch#
```

This example shows how to display ONVIF-based NVR information associated with the group ID 'ipc-list'.

```
Switch# show surveillance vlan onvif-nvr interface eth1/0/1 ipc-list

Interface IP Address      MAC address       Group    Description
--------- --------------- ----------------- -------- -----------------
1         10.90.90.90.1   00-01-02-03-04-05 1        D-Link-IPC-1
1         10.90.90.90.2   00-01-02-03-04-06 1        D-Link-IPC-2

Total Entries: 2

Switch#
```

61. Switch Port Commands

61-1 duplex

This command is used to configure the duplex mode setting of the physical port. Use the **no** form of command to revert to the default setting.

duplex {full | auto}

no duplex

Parameters

full	Specifies that the port operates in the full-duplex mode.
auto	Specifies that the port's duplex mode will be determined by auto-negotiation.

Default

By default, the duplex is **auto** for the 10G copper ports.

By default, the duplex is **full** for the 10G SFP+ ports and 25G SFP28 ports.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to configure the duplex mode setting of the physical port.

Example

This example shows how to configure port 1 to operate at a forced speed of 100Mbits and specifies that the duplex mode should be set to auto-negotiated.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

61-2 flowcontrol

This command is used to configure the flow control capability of the port interface. Use the **no** form of command to revert to the default setting.

flowcontrol {on | off}

no flowcontrol

Parameters

on	Specifies to enable a port to send PAUSE frames or process PAUSE frames from remote ports.
off	Specifies to disable the ability for a port to send or receive PAUSE frames.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command can only assure that the flow control capability has been configured in the Switch software and not guarantee the actual hardware operation. The actual hardware operation may be different to the settings that have been configured on the Switch because the flow control capability is determined by both the local port/device and the device connected at the other end of the link, not just by the local device.

If the speed is set to the forced mode, the final flow control setting will be determined by the configured flow control setting. If the speed is set to the auto mode, the final flow control setting will be based on the negotiated result between the local side setting and the partner side setting. The configured flow control setting here is the local side setting.

Example

This example shows how to enable the flow control on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# flowcontrol on
Switch(config-if)#
```

61-3 mdix

This command is used to configure the port Media-Dependent Interface Crossover (MDIX) state. Use the **no** form of command to revert to the default setting.

mdix {auto | normal | cross}

no mdix

Parameters

auto	Specifies to set the port interface's MDIX state to the auto-MDIX mode.
normal	Specifies to force the port interface's MDIX state to the normal mode.
cross	Specifies to force the port interface's MDIX state to the cross mode.

Default

By default, this option is set as **auto**.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command cannot be applied to a port when the medium of the port interface is fiber.

Example

This example shows how to configure the MDIX state auto on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mdix auto
Switch(config-if)#
```

61-4 speed

This command is used to configure the physical port interface's speed settings. Use the **no** form of command to revert to the default setting.

speed {100 | 1000 | 10giga | 25giga | auto [*SPEED-LIST***]}**

no speed

Parameters

100	Specifies to force the speed to 100 Mbps.
1000	Specifies to force the speed to 1000 Mbps.
10giga	Specifies to force the speed to 10 Gbps.
25giga	Specifies to force the speed to 25 Gbps.
auto	Specifies to determine the speed and flow control via auto-negotiation with its link partner.
SPEED-LIST	(Optional) Specifies a list of speeds that the Switch will only auto-negotiate to. The speed can be **100**, **1000**, and/or **10giga**. Use a comma (,) to separate multiple speeds. If the speed list is not specified, all speeds will be advertised.

Default

By default, the speed is **auto** for the 10G copper ports and 10G SFP+ ports.

By default, the speed is **25giga** for the 25G SFP28 ports.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

Auto-negotiation should be enabled on the 10G copper ports. Auto-negotiation is not supported for the 25G fiber ports. For DXS-1210-28T, ports 25 to 28 must operate at the same speed.

If the specified speed is not supported by the hardware, error messages will be returned.

NOTE: The FEC function is not supported on the 25 Gbps SFP28 ports. If the 25 Gbps SFP28 connection between this switch and another non-DXS-1210 series switch is not working, the FEC function needs to be disabled on the remote switch.

Example

This example shows how to configure port 1 to only auto-negotiate to 100Mbps or 1000Mbps.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# speed auto 100,1000
Switch(config-if)#
```

62. System File Management Commands

62-1 boot config

This command is used to specify the file that will be used as the configuration file for the next boot.

boot config {Config1 | Config2}

Parameters

Config1	Specifies to use Config1 as the startup configuration file.
Config2	Specifies to use Config2 as the startup configuration file.

Default

By default, Config1 is used.

Command Mode

Global Configuration Mode.

Usage Guideline

The command is used to specify the startup configuration file. If there is no valid configuration file, the device will be configured to the default state.

Example

This example shows how to configure the file “Config2” as the startup configuration file.

```
Switch#configure terminal
Switch(config)#boot config Config2
Switch(config)#
```

62-2 boot image

This command is used to specify the file that will be used as the image file for the next boot.

boot image [check] {Image1 | Image2}

Parameters

check	(Optional) Specifies to display the firmware information for the specified file. This information includes the version number and model description.
Image1	Specifies to use Image1 as the boot image file.
Image2	Specifies to use Image2 as the boot image file.

Default

By default, Image1 is the boot image.

Command Mode

Global Configuration Mode.

Usage Guideline

When using the **boot image** command, the associated specified boot image file will be the startup boot image file for the next reboot. Use this command to assign a file as the next-boot image file. The system will check the model and checksum to determine whether the file is a valid image file.

The purpose of the **check** parameter is for checking the file information to let the user understand whether the specified file is suitable to be a boot image or not. The setting of the **boot image** command will immediately be stored in the NVRAM, which is a space separated from the start-up configuration.

Example

This example shows how to specify that the Switch should use the image file named “Image1” as the boot image file for the next startup.

```
Switch#configure terminal
Switch(config)#boot image Image1
Switch(config)#
```

62-3 clear running-config

This command is used to clear the system’s running configuration.

clear running-config

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the system’s configuration retained in DRAM. The configuration data will revert to the default settings. Before using this command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.

This command will clear the system’s configuration settings, including IP parameters. Thus, all the existing remote connections will be disconnected. After this command was applied, the user needs to setup the IP address via the local console.

Example

This example shows how to clear the system’s running configuration.

```
Switch#clear running-config

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear running configuration? (y/n) [n]  y


Switch#
```

62-4 reset system

This command is used to reset the system, clear the system's configuration, then save and reboot the Switch.

reset system

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to clear the system's configuration. The configuration data will revert to the default settings and then save it to the start-up configuration file and then reboot switch. Before using this command, save a backup of the configuration using the copy command or upload the configuration profile to the TFTP server.

Example

This example shows how to reset the system to the factory default settings.

```
Switch# reset system

This command will clear the system's configuration to the factory
default settings, including the IP address.
Clear system configuration, save, reboot? (y/n) [n]  y

Saving configurations and logs to NV-RAM...... Done.
Please wait, the switch is rebooting...
```

62-5 configure replace

This command is used to replace the current running configuration with the indicated configuration file.

configure replace {{tftp: *//LOCATION/FILENAME* **| flash: {Config1 | Config2}} [force]**

Parameters

tftp:	Specifies that the configuration file is from the TFTP server.
//LOCATION/FILENAME	Specifies the URL of the configuration file on the TFTP server.
flash:	Specifies that the configuration file is from the NVRAM of the device.
Config1	Specifies the Config1 file as the boot config file.
Config2	Specifies the Config2 file as the boot config file.
force	(Optional) Specifies to execute the command immediately with no confirmation needed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to execute the indicated configuration file to replace the current running configuration. The current running configuration will be cleared before applying the indicated configuration.

NOTE: The command will replace the current running configuration with the contents of the specified configuration file. So the specified configuration file is assumed to be a complete configuration, not a partial configuration.

Before using the **configure replace** command, save a backup of the configuration using the **copy** command or upload the configuration profile to the TFTP server.

Example

This example shows how to download the “config.cfg” from the TFTP server and replace the current running configuration with it.

```
Switch# configure replace tftp: //10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing tftp://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to replace the current running configuration with the “Config1” file stored in the NVRAM of the device. Execute the command immediately without confirmation.

```
Switch#configure replace flash: Config1 force

 Executing script file Config1 ......
 Executing done

Switch#
```

62-6 copy

This command is used to copy a file to another file.

copy *SOURCE-URL DESTINATION-URL*

copy *SOURCE-URL* **tftp: [***I**LOCATIONIDESTINATION-URL***]**

copy tftp: [*I**LOCATIONISOURCE-URL***]** *DESTINATION-URL*

Parameters

SOURCE-URL	Specifies the source URL for the source file to be copied. One special form of the URL is represented by the following keywords. If **startup-config** is specified as the *SOURCE-URL*, the purpose is to upload the startup configuration, save the startup configuration as the file in the file system, or to execute the startup configuration as the running configuration. If **running-config** is specified as the *SOURCE-URL*, the purpose is to upload the running configuration or save the running configuration as the startup configuration or to save it as the file in the file system. If **flash: [***PATH-FILE-NAME***]** is specified as the *SOURCE-URL*, the purpose is to specify the source file to be copied in the file system. If **log** is specified as the *SOURCE-URL*, the system log can be retrieved to the TFTP server. If **attack-log** is specified as the *SOURCE-URL*, the purpose is to upload the attack log.
DESTINATION-URL	Specifies the destination URL for the copied file. One special form of the URL is represented by the following keywords. If **running-config** is specified as the *DESTINATION-URL*, the purpose is to apply a configuration to the running configuration. If **startup-config** is specified as the *DESTINATION-URL*, the purpose is to save a configuration to the next-boot configuration. That is to keep the current configuration into the NVRAM and the file name will be the same as the file name specified with the **boot config** command. If **flash: {Image1 | Image2 | Config1 | Config2}** is specified as the *DESTINATION-URL*, the purpose is to specify the copied file in the file system. If **flash: certificate-key** *STRING* is specified as the *DESTINATION-URL*, the purpose is to specify the destination certificate file or key file to be copied in the file system. If **flash: private-key** *STRING* is specified as the *DESTINATION-URL*, the purpose is to specify the destination private key file to be copied in the file system. If **flash: public-key** *STRING* is specified as the *DESTINATION-URL*, the purpose is to specify the destination public key file to be copied in the file system.
LOCATION	(Optional) Specifies the IPv4/IPv6 address of the TFTP server.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to copy a file to another file in the file system. Use this command to download or upload the configuration file or the image file. To upload the running configuration or save the running configuration to the startup configuration, specify **running-config** as the *SOURCE-URL*. To save the running configuration to the startup configuration, specify **startup-config** as the *DESTINATION-URL*.

As the destination is the startup configuration, the source file is directly copied to the file specified in the **boot config** command. Thus the original startup configuration file will be overwritten.

To apply a configuration file to the running configuration, specify **running-config** as the *DESTINATION-URL* for the **copy** command and the configuration file will be executed immediately by using the increment method. That means that the specified configuration will merge with the current running configuration. The running configuration will not be cleared before applying of the specified configuration.

As the specified source is the system log and the specified destination is a URL, the current system log will be copied to the specified URL.

To represent a file in the remote TFTP server, the URL must be prefixed with “tftp: //”.

To download the firmware image, the user should use the **copy tftp: //** command to download the file from the TFTP server to a file in the file system. Then, use the **boot image** command to specify it as the boot image file.

Example

This example shows how to configure the Switch’s running configuration by using the increment method using the configuration called “switch-config.cfg” that is download from the TFTP server 10.1.1.254.

```
Switch#copy tftp: //10.1.1.254/switch-config.cfg running-config

Address of remote host [10.1.1.254]?
Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Accessing tftp://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 29974 bytes.
 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

This example shows how to upload the running configuration to the TFTP server for storage.

```
Switch#copy running-config tftp: //10.1.1.254/switch-config.cfg

Address of remote host [10.1.1.254]?
Destination filename [switch-config.cfg]?
 Accessing tftp://10.5.2.101/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 28999 bytes.

Switch#
```

This example shows how to save the system’s running configuration into the flash memory and uses it as the next boot configuration.

```
Switch#copy running-config startup-config

Destination filename startup-config? [y/n]:  y

Saving all configurations to NV-RAM..... Done.

Switch#
```

This example shows how to execute the “Config2” file in the NVRAM immediately by using the increment method.

```
Switch#copy flash: Config2 running-config

Source filename [Config2]?
Destination filename running-config? [y/n]:  y

 Executing script file Config2 ......
 Executing done

Switch#
```

This example shows how to download an image file from the TFTP server.

```
Switch#copy tftp: //10.1.1.254/runtime.had flash: Image1

Address of remote host [10.1.1.254]?
Source filename [dxs-1210.had]?
Destination filename [Image1]?
 Accessing tftp://10.1.1.254/runtime.had...
 Transmission start...
 Transmission finished, file length 8315060 bytes.
 Please wait, programming flash.............. Done.

Switch#
```

62-7 reboot

This command is used to reboot the Switch.

reboot [force_agree]

Parameters

force_agree	(Optional) Specifies to restart the Switch without confirmation.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is used to reboot the Switch.

Example

This example shows how to reboot the Switch.

```
Switch# reboot force_agree

Please wait, the switch is rebooting...
```

62-8 show boot

This command is used to display the boot configuration file and the boot image setting.

show boot

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is used to display the boot configuration file and the boot image setting.

Example

This example shows how to display system boot information.

```
Switch#show boot

 Boot image: /c:/Image1
 Boot config: /c:/Config1


Switch#
```

62-9 show running-config

This command is used to display the commands in the running configuration file.

show running-config [effective | all] [interface *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Parameters

effective	(Optional) Specifies to display command configurations that affected the behavior of the Switch. For example, if STP was disabled, only the **disable stp** command will be displayed. All other lower layer settings regarding STP will not be displayed. The lower layer settings will only be displayed when the higher layer setting is enabled. Only modified configurations different from the default configuration will be displayed if this option is not selected.

all	(Optional) Specifies to display all command configurations; including commands corresponding with the default parameters. Only modified configurations different from the default configuration will be displayed if this option is not selected. interface INTERFACE-ID
interface *INTERFACE-ID*	(Optional) Specifies the interface to be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the current running system configuration.

Example

This example shows how to display the content of the running configuration file.

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

Current configuration : 1291 bytes

!----------------------------------------------------------------------------
!             DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch
!                               Configuration
!
!                             Firmware: Build 1.00.021
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

line console
!
line telnet
!
line ssh
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
!
interface Ethernet1/0/3
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a Alll
```

62-10 show startup-config

This command is used to display the content of the startup configuration file.

show startup-config

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the configuration settings that the system will be initialized with.

Example

This example shows how to display the content of the startup configuration file.

```
Switch#show startup-config

!----------------------------------------------------------------------------
!             DXS-1210-28T 10 Gigabit Ethernet Smart Managed Switch
!                               Configuration
!
!                             Firmware: Build 1.00.021
!           Copyright(C) 2020 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

ip http timeout-policy idle 36000
!
line console
 session-timeout 0
!
line telnet
!
line ssh
!
interface Ethernet1/0/1
!
interface Ethernet1/0/2
!
interface Ethernet1/0/3
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

63. System Log Commands

63-1 clear logging

This command is used to delete log messages in the system logging buffer.

clear logging

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to delete all the log messages in the system logging buffer.

Example

This example shows how to delete all the log messages in the logging buffer.

```
Switch#clear logging
Clear logging? (y/n) [n]  y
Switch#
```

63-2 logging on

This command is used to enable the logging of system messages. Use the **no** form of this command to disable the logging of system messages.

logging on

no logging on

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the logging of system messages. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or the syslog server. System logging messages are also known as system error messages. Logging can be turned on and off for these destinations individually using the **logging buffered**, **logging server**, and **logging console** commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. If the **logging on** command is enabled, the logging buffered will be enabled at the same time.

Example

This example shows how to enable the logging of system messages.

```
Switch# configure terminal
Switch(config)# logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

63-3 logging buffered

This command is used to enable logging of system messages to the local message buffer. Use the **no** form of this command to disable the logging of messages to the local message buffer. Use the **default logging buffered** command to revert to default setting.

logging buffered [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***] [write-delay {***SECONDS* **| infinite}]**

no logging buffered

default logging buffered

Parameters

SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. If not specified, the default severity level is warnings (4).
SEVERITY-NAME	(Optional) Specifies the severity level of system messages by one of the following names: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**.
discriminator	(Optional) Specifies to filter the message to be sent to local buffer based on the discriminator.
write-delay *SECONDS*	(Optional) Specifies to disable periodical writing of the logging buffer to the FLASH.

Default

By default, the severity level is warning (4).

Command Mode

Global Configuration Mode.

Usage Guideline

The system messages can be logged to the local message buffer or to other destinations. Messages must enter the local message buffer first before it can be further dispatched to other destinations.

This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.

Specify the severity level of the messages in order to restrict the system messages that are logged in the logging buffer (thus reducing the number of messages logged). The messages which are at the specified severity level or

higher will be logged to the message buffer. When the logging buffer is full, the oldest log entries will be removed to create the space needed for the new messages that are logged.

The content of the logging buffer will be saved to the FLASH memory periodically such that the message can be restored on reboot. The interval for periodically writing the logging buffer to FLASH can be specified. The content of the logged messages in the FLASH will be reloaded into the logging buffer on reboot.

Example

This example shows how to enable the logging of messages to the logging buffer and restrict logging of messages with a security level of errors or higher.

```
Switch# configure terminal
Switch(config)# logging buffered severity errors
Switch(config)#
```

63-4 logging console

This command is used to enable the logging of system messages to the local console. Use the **no** form of this command to disable the logging of messages to the local console and revert to the default setting.

logging console [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

no logging console

Parameters

SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Optional) Specifies to filter the message to be sent to the local console based on the discriminator.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

The system messages can be logged to the local message buffer, local console or other destinations. Messages must enter the local message buffer first before it can further be dispatched to the console.

This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied.

Specify the severity level of the messages in order to restrict the system messages that are logged to the console. The messages which are at the specified severity level or higher will be dispatched to the local console.

Example

This example shows how to enable the logging of messages to the local console and restrict the logging of messages with a security level of errors or higher.

```
Switch# configure terminal
Switch(config)# logging console severity errors
Switch(config)#
```

63-5 logging discriminator

This command is used to create a discriminator that can be further used to filter SYSLOG messages sent to various destinations. Use the **no** form of this command to remove the discriminator.

logging discriminator *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

no logging discriminator *NAME*

Parameters

NAME	Specifies the name of the discriminator.
facility	(Optional) Specifies a sub-filter based on the facility string.
STRING	Specifies one or more facility names. If multiple facility names are used, they should be separated by commas without spaces before and after the comma.
includes	Specifies to include the matching message. The unmatched messages are filtered.
drops	Specifies to filter the matching message.
severity	(Optional) Specifies a sub-filter based on severity matching.
SEVERITY-LIST	Specifies a list of severity levels to be filtered or to be included.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

An existing discriminator can be configured. The later setting will overwrite the previous setting. Associate a discriminator with the logging buffered and the logging server command.

Example

This example shows how to create a discriminator named “buffer-filter” which specifies two sub-filters, one based on the severity level and the other based on the facility.

```
Switch# configure terminal
Switch(config)# logging discriminator buffer-filter facility includes STP severity includes 1-4,6
Switch(config)#
```

63-6 logging server

This command is used to create a SYSLOG server host to log the system messages or debug output. Use the **no** form of this command to remove a SYSLOG server host.

logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility {***FACILITY-NUM* **|** *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

no logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IP address of the SYSLOG server host.
IPV6-ADDRESS	Specifies the IPv6 address of the log server host.
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to the log server. This value must be between 0 and 7. 0 is the most severe level. If not specified, the default severity level is warnings (4).
SEVERITY-NAME	(Optional) Specifies the severity level of system messages by one of the following names: **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, and **debugging**.
FACILITY-NUM	(Optional) Specifies a decimal value from 0 to 23 to represent the facility. If not specified, the default facility is local7 (**23**). See the usage guideline for more information.
FACILITY-NAME	(Optional) Specifies a facility name to represent the facility. If not specified, the default facility is **local7** (23). See the usage guideline for more information.
discriminator *NAME*	(Optional) Specifies to filter the message to the log server based on discriminator.
port *UDP-PORT*	(Optional) Specifies the UDP port number to be used for the SYSLOG server. Valid values are 514 (the IANA well-known port) or any value from 1024 to 65535. If not specified, the default UDP port is 514.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

System messages can be logged to the local message buffer, local console or remote hosts. Messages must enter the local message buffer first before it can be further dispatched to logging server.

The following is a table for the facility.

Numerical code	Facility
0	Kernel messages.
1	User-level messages.
2	Mail system.
3	System daemons.
4	Security/authorization messages.
5	Messages generated internally by the SYSLOG.
6	Line printer sub-system.

7	Network news sub-system.
8	UUCP sub-system.
9	Clock daemon.
10	Security/authorization messages.
11	FTP daemon.
12	NTP subsystem.
13	Log audit.
14	Log alert.
15	Clock daemon (note 2).
16	Local use 0 (local0).
17	Local use 1 (local1).
18	Local use 2 (local2).
19	Local use 3 (local3).
20	Local use 4 (local4).
21	Local use 5 (local5).
22	Local use 6 (local6).
23	Local use 7 (local7).

Example

This example shows how to enable the logging of system messages with a severity higher than warnings to the remote host 20.3.3.3.

```
Switch# configure terminal
Switch(config)# logging server  20.3.3.3 severity warnings
Switch(config)#
```

63-7 show logging

This command is used to display the system messages logged in the local message buffer.

show logging [all | [*REF-SEQ***] [+** *NN* **| -** *NN***]]**

Parameters

all	Specifies to display all log entries starting from the latest message.
REF-SEQ	Specifies to start the display from the reference sequence number.
+ *NN*	Specifies the number of messages that occurred after the specified reference sequence number. If the reference index is not specified, it starts from the eldest message in the buffer.
- *NN*	Specifies the number of messages that occurred prior to the specified reference sequence number. If the reference index is not specified, the message display starts from the last message written in the buffer.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the system messages logged in the local message buffer.

Each message logged in the message buffer is associated with a sequence number. As a message is logged, a sequence number starting from 1 is allocated. The sequence number will roll back to 1 when it reaches 100000.

When the user specifies to display a number of messages following the reference sequence number, the oldest messages are displayed prior to the newer messages. When the user specifies to display a number of messages prior to the reference sequence number, the newer messages are displayed prior to the later messages.

If the command is issued without options, the system will display up to 200 entries starting from the latest message.

Example

This example shows how to display the messages in the local message buffer.

```
Switch# show logging

Total number of buffered messages: 2

#2 2013-08-02 16:37:36 INFO(6) Logout through Console (Username: Anonymous)
#1 2013-08-02 16:35:54 INFO(6) Port eth1/0/1 link up, 1000Mbps FULL duplex

switch#
```

63-8 show attack-logging

This command is used to display attack log messages.

show attack-logging [index *INDEX***]**

Parameters

index*INDEX*	(Optional) Specifies the list of index numbers of the entries that need to be displayed. If no index is specified, all entries in the attack log DB will be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the attack log messages. The attack log message refers to log messages driven by modules such as DOS and the port-security module. This type of log message may generate a large amount of messages and quickly cause the system to run out of system log storage. Therefore, for this type of log messages only the first log that is generated each minute can be stored in the system log, with the rest of them being stored in a separate table named attack log.

Example

This example shows how to display the first attack log entry.

```
Switch#show attack-logging

Attack log messages (total number:0)


Switch#
```

63-9 clear attack-logging

This command is used to delete the attack log.

clear attack-logging {all}

Parameters

all	Specifies to clear all attack log entries.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command used to delete the attack log messages.

Example

This example shows how to delete all the attack log messages.

```
Switch# clear attack-logging all
Switch#
```

64. Time and SNTP Commands

64-1 clock set

This command is used to manually set the system's clock.

clock set *HH:MM:SS DAY MONTH YEAR*

Parameters

HH:MM:SS	Specifies the current time in hours (24-hour format), minutes and seconds.
DAY	Specifies the current day (by date) in the month.
MONTH	Specifies the current month (by name, jan, feb, mar, apr, and so on).
YEAR	Specifies the current year (no abbreviation).

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Generally, if the system is synchronized by a valid outside timing mechanism, such as SNTP, there is no need to set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the clock timezone command. The clock configured by this command will be applied to RTC if it is available. The configured clock will not be stored in the configuration file.

If the clock is manually set and the SNTP server is configured, the system will still try to sync the clock with the server. If the clock is manually set, but a new clock time is obtained by the SNTP server, the clock will be replaced by the new synced clock.

Example

This example shows how to manually set the software clock to 6:00 p.m. on Jul. 4, 2020.

```
Switch# clock set 18:00:00 4 jul 2020
Switch#
```

64-2 clock summer-time

This command is used to configure the system to automatically switch to summer time (daylight saving time). Use the **no** form of this command to configure the Switch to not automatically switch over to summer time.

clock summer-time recurring *WEEK DAY MONTH HH:MM WEEK DAY MONTH HH:MM* **[***OFFSET***]**

clock summer-time date *DATE MONTH YEAR HH:MM DATE MONTH YEAR HH:MM* **[***OFFSET***]**

no clock summer-time

Parameters

recurring	Specifies that summer time should start and end on the specified week day of the specified month.

date	Specifies that summer time should start and end on the specified date of the specified month.
WEEK	Specifies the week of the month (1 to 4 or last).
DAY	Specifies the day of the week (sun, mon, and so on).
DATE	Specifies the date of the month (1 to 31).
MONTH	Specifies the month (by name, jan, feb, mar, apr, and so on).
YEAR	Specifies the start and end years for the summer time data.
HH:MM	Specifies the time (24 hours format) in hours and minutes.
OFFSET	(Optional) Specifies the number of minutes to add during summer time. The default value is 60. The range of this offset is 30, 60, 90 and 120.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to automatically switch over to summer time. The command has two forms. One is the recurring form which is used to specify the time through the week and the day of the month. The other form is the date form which is used to specify the date of the month.

In both the date and recurring forms of the command, the first part of the command specifies when summer time begins, and the second part specifies when it ends.

Example

This example shows how to specify that summer time starts on the first Sunday in June at 2 a.m. and ends on the last Sunday in October at 2 a.m.

```
Switch# configure terminal
Switch(config)# clock summer-time recurring 1 sun jun 2:00 last sun oct 2:00
Switch(config)#
```

64-3 clock timezone

This command is used to set the time zone for display purposes. Use the **no** form of this command to revert to the default setting.

clock timezone {+ | -} *HOURS-OFFSET* **[***MINUTES-OFFSET***]**

no clock timezone

Parameters

+ | -	Specifies that time to be added to the UTC.
-	Specifies that time to be subtracted from the UTC.
HOURS-OFFSET	Specifies the hours difference from UTC.
MINUTES-OFFSET	(Optional) Specifies the minutes difference from UTC.

Default

By default, this option is set to UTC.

Command Mode

Global Configuration Mode.

Usage Guideline

The time obtained by the SNTP server refers to the UTC time. The local time will be calculated based on UTC time, time zone, and the daylight saving configuration.

Example

This example shows how to set the time zone to the Pacific Standard Time (PST), which is 8 hours behind of UTC.

```
Switch# configure terminal
Switch(config)# clock timezone - 8
Switch(config)#
```

64-4 show clock

This command is used to display the time and date information.

show clock

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command also indicates the clock's source. The clock source can be "No Time Source" or "SNTP".

Example

This example shows how to display the current time.

```
Switch# show clock

     Current Time Source   : System Clock
     Current Time          : 05:56:45, 2000-01-01
     Time Zone             : UTC +00:00
     Daylight Saving Time  : Disabled

Switch#
```

64-5 show sntp

This command is used to display information about the SNTP server.

show sntp

Parameters

None.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display information about the SNTP server.

Example

This example shows how to display SNTP information.

```
Switch#show sntp

SNTP Status               : Enabled
SNTP Poll Interval        : 720 sec

SNTP Server Status:

SNTP Server                                    Version Last Receive
---------------------------------------------- ------- ---------------
172.31.151.44                                  3       00:00:29 Synced
172:31:151:24::44                              ------- ---------------
FE80::41A2:ACB6:9B9E:C5D4%vlan40               ------- ---------------
---------------------------------------------- ------- ---------------
Total Entries:3


Switch#
```

64-6 sntp server

This command is used to allow the system clock to be synchronized with an SNTP time server. Use the **no** form of this command to remove a server from the list of SNTP servers.

sntp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

no sntp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IP address of the time server which provides the clock synchronization.

IPV6-ADDRESS	pecifies the IPv6 address of the time server.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

SNTP is a compact, client-only version of the NTP. Unlike NTP, SNTP can only receive the time from NTP servers; it cannot be used to provide time services to other systems. SNTP typically provides time within 100 milliseconds of the accurate time, but it does not provide the complex filtering and statistical mechanisms of NTP. In addition, SNTP does not authenticate traffic, although you can configure extended access lists to provide some protection.

Create multiple SNTP servers by enter this command multiple times with different SNTP server IP addresses.

Use the **no** form of this command to delete the SNTP server entry. To delete an entry, specify the information exactly the same as the originally configured setting. The time obtained from the SNTP server refers to the UTC time.

Example

This example shows how to configure a switch to allow its software clock to be synchronized with the clock by the SNTP server at IP address 192.168.22.44.

```
Switch# configure terminal
Switch(config)# sntp server 192.168.22.44
Switch(config)#
```

64-7 sntp enable

This command is used to enable the SNTP function. Use the **no** form of this command to disable the SNTP function.

sntp enable

no sntp enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable or disable the SNTP function.

Example

This example shows how to enable the SNTP function.

```
Switch# configure terminal
Switch(config)# sntp enable
Switch(config)#
```

64-8 sntp interval

This command is used to set the interval for the SNTP client to synchronize its clock with the server. Use the **no** form of this command to revert to the default setting.

sntp interval *SECONDS*

no sntp interval

Parameters

SECONDS	Specifies the synchronization interval from 30 to 99999 seconds.

Default

By default, this value is 720 seconds.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to set the polling interval.

Example

This example shows how to configure the interval to 100 seconds.

```
Switch# configure terminal
Switch(config)# sntp interval 100
Switch(config)#
```

65. Time Range Commands

65-1 periodic

This command is used to specify the period of time for a time range profile. Use the **no** form of this command to remove the specified period of time.

periodic {daily *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

no periodic {daily *HH:MM* **to H***H:MM* **| weekly** *WEEKLY-DAY* **H***H:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

Parameters

daily *HH:MM* **to H***H:MM*	Specifies the time of the day, using the format HH:MM (for example, 18:30).
weekly *WEEK-DAY HH:MM* **to [***WEEK-DAY***]** *HH:MM*	Specifies the day of the week and the time of day in the format day HH:MM, where the day of the week is spelled out (monday, tuesday, wednesday, thursday, friday, saturday, and sunday). If the ending day of the week is the same as the starting day of the week, it can be omitted.

Default

None.

Command Mode

Time-range Configuration Mode.

Usage Guideline

A new period can be partially overlapped with an older one. If a new period's starting and ending time is respectively the same as a previous period, an error message will be displayed and the new period will not be allowed. When specifying a period to remove, it must be the same period originally added and cannot be a partial range of a period or multiple periods configured. Otherwise, an error message will be displayed.

Example

This example shows how to create a time-range that include daily 09:00 to 12:00, 00:00 Saturday to 00:00 Monday and delete the period for daily 09:00 to 12:00.

```
Switch# configure terminal
Switch(config)# time-range rdtime
Switch(config-time-range)# periodic daily 9:00 to 12:00
Switch(config-time-range)# periodic weekly saturday 00:00 to monday 00:00
Switch(config-time-range)# no periodic daily 9:00 to 12:00
Switch(config-time-range)#
```

65-2 show time-range

This command is used to display the time range profile configuration.

show time-range [*NAME***]**

Parameters

NAME	(Optional) Specifies the name of the time-range profile to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all configured time-range profiles will be displayed.

Example

This example shows how to display all the configured time ranges.

```
Switch# show time-range

Time Range Profile: rdtime
Daily 09:00 to 12:00
Weekly Saturday 00:00 to Monday 00:00

Time Range Profile: lunchtime
Daily 12:00 to 13:00

Total Entries: 2

Switch#
```

65-3 time-range

This command is used to enter the Time-range Configuration Mode to define a time range. Use the **no** form of this command to delete a time range.

time-range *NAME*

no time-range *NAME*

Parameters

NAME	Specifies the name of the time-range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the Time-range Configuration Mode before using the **periodic** command to specify a time period. When a time-range is created without any time interval (periodic) setting, it implies that there is not any active period for the time-range.

Example

This example shows how to enter the Time-range Configuration Mode for the time-range profile, named “rdtime”.

```
Switch# configure terminal
Switch(config)# time-range rdtime
Switch(config-time-range)#
```

66. Traffic Segmentation Commands

66-1 show traffic-segmentation forward

This command is used to display the traffic segmentation for ports.

show traffic-segmentation forward [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

This command is only available for physical port and port-channel interface configuration.

If no parameter is specified, the traffic segmentation configuration for all ports is displayed.

Example

This example shows how to display the configuration of traffic segmentation on port 1.

```
Switch# show traffic-segmentation forward interface eth1/0/1

Interface        Forwarding Domain
-------------    ------------------------------------------------------------
eth1/0/1         eth1/0/2,1/0/4-1/0/6

Total Entries: 1

Switch#
```

66-2 traffic-segmentation forward

This command is used to restrict the Layer 2 packet forwarding domain of packets received by the configured port. Use the **no** form of this command to remove the specification of forwarding domain.

traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

no traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the interfaces to be configured.

,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command is only available for physical port interface configuration.

When traffic segmentation forwarding domain is specified, packets received by the port will be restricted in Layer 2 packet forwarding to interfaces within the domain. When the forwarding domain of a port is empty, Layer 2 forwarding for packets received by the port is not restricted.

The **traffic-segmentation forward** command can be entered multiple times. The following interfaces will be appended into the forwarding domain. Use the **no** form of this command to remove the specified interface from the traffic segmentation forward member list.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, there is no restriction on Layer 2 forwarding of packets received by the port.

Example

This example shows how to This example shows how to configure traffic segmentation. It restricts the flooding domain of port 1 to the range of ports 3 to 6.

```
Switch# configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#traffic-segmentation forward interface eth1/0/3-6
Switch(config-if)#
```

67. Transport Layer Security (TLS) Commands

67-1 no certificate

This command is used to delete the imported certificate.

no certificate *NAME*

Parameters

NAME	Specifies the name of the certificate to be deleted.

Default

None.

Command Mode

Certificate Chain Configuration Mode.

Usage Guideline

Use the **show crypto pki trustpoints** command to get a name list of imported certificates. Then, use this command to delete the imported certificates of a trust point. If the specified certificate is a local certificate, the corresponding private key will be deleted at the same time. A warning message will be displayed when a private key is to be deleted.

Example

This example shows how to delete an imported certificate named tongken.ca of the trust point gaa.

```
Switch# show crypto pki trustpoints

Trustpoint Name        : gaa (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Switch# configure terminal
Switch(config)# crypto pki certificate chain gaa
Switch(config-cert-chain)# no certificate tongken.ca
Switch(config-cert-chain)#
```

67-2 crypto pki import pem

This command is used to import the CA certificate or the Switch certificate and keys to a trust-point from privacy-enhanced mail (PEM)-formatted files.

crypto pki import *TRUSTPOINT* **pem** *FILE-SYSTEM*:**/[***DIRECTORY***/]***FILE-NAME* **[password** *PASSWORD-PHRASE***] {ca | local | both}**

crypto pki import *TRUSTPOINT* **pem tftp://***IP-ADDRESS***/[***DIRECTORY***/]***FILE-NAME* **[password** *PASSWORD-PHRASE***] {ca | local | both}**

Parameters

TRUSTPOINT	Specifies the name of the trust-point that is associated with the imported certificates and key pairs.
FILE-SYSTEM	Specifies the file system for certificates and key pairs. A colon (:) is required after the specified file system. For example, **flash:** represents the system FLASH.
DIRECTORY	(Optional) Specifies the directory name where the Switch should import the certificates and key pairs in the Switch or TFTP server.
FILE-NAME	Specifies the name of the certificates and key pairs to be imported. By default, the Switch will append this name with *.ca*, *.prv* and *.crt* for CA certificate, private key and certificate respectively.
password *PASSWORD-PHRASE*	(Optional) Specifies the encrypted password phrase that is used to undo encryption when the private keys are imported. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
tftp:	Specifies the source URL for a TFTP network server.
IP-ADDRESS	Specifies the IP address of the TFTP server.
ca	Specifies to import the CA certificate only.
local	Specifies to import local certificate and key pairs only.
both	Specifies to import the CA certificate, local certificate and key pairs.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to import certificates and key pairs in the PEM-formatted files.

Proper certificates and key pairs need to be imported to the Switch according to the desired key exchange algorithm. RSA and DSA certificates/key pairs should be imported for RSA and DHS-DSS respectively. RSA and DSA certificates and keys are incompatible. An SSL client that has only an RSA certificate and key cannot establish a connection with an SSL server that has only a DSA certificate and key.

The imported certificate(s) may form a certificate chain which establishes a sequence of trusted certificates from a peer certificate to the root CA certificate. The trust point CA is the certificate authority configured on the Switch as the trusted CA. Any obtained peer certificate will be accepted if it is signed by a locally trusted CA or its subordinates.

If the specified trust point does not exist, an error message will be prompted.

Example

This example shows how to import certificates (CA and local) and key pair files to trust-point "TP1" via TFTP.

```
Switch# configure terminal
Switch(config)# crypto pki import TP1 pem tftp: //10.1.1.2/name/msca password abcd1234 both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via eth1/0/5):!
[OK - 1082 bytes]

% Importing private key PEM file...
Reading file from tftp://10.1.1.2/name/msca.prv
Loading name/msca.prv from 10.1.1.2 (via eth1/0/5):!
[OK - 573 bytes]

% Importing certificate PEM file...
Reading file from tftp://10.1.1.2/name/msca.crt
Loading name/msca.crt from 10.1.1.2 (via eth1/0/5):!
[OK - 1289 bytes]
% PEM files import succeeded.

Switch(config)#
```

67-3 crypto pki trustpoint

This command is used to declare the trust-point that the Switch will use. Use the **no** form of this command to delete all certificates and key pairs associated with the trust-point.

crypto pki trustpoint *NAME*

no crypto pki trustpoint *NAME*

Parameters

NAME	Specifies to create a name for the trust-point.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to declare a trust-point, which can be a self-signed root certificate authority (CA) or a subordinate CA. Issuing this command will enter the CA-Trust-Point Configuration Mode.

Example

This example shows how to declare a trust-point "TP1" and specify it is a primary trust-point.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

67-4 crypto pki certificate chain

This command is used to enter the Certificate Chain Configuration Mode.

crypto pki certificate chain *NAME*

Parameters

NAME	Specifies the name for the trust-point.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enter the Certificate Chain Configuration Mode. If the specified trust-point name does not exist, an error message will be displayed.

Example

This example shows how to enter the Certificate Chain Configuration Mode.

```
Switch# configure terminal
Switch(config)# crypto pki certificate chain TP1
Switch(config-cert-chain)#
```

67-5 primary

This command is used to assign a specified trustpoint as the primary trustpoint of the Switch. Use the **no** form of this command to unbind the setting.

primary

no primary

Parameters

None.

Default

By default, this option is disabled.

Command Mode

CA-Trust-Point Configuration Mode.

Usage Guideline

Use this command to specify a given trust-point as primary. This trust-point can be used as default trust-point when the application does not explicitly specify which certificate authority (CA) trust-point should be used. Only one trust-point can be specified as the primary. The last trust-point specified as the primary will overwrite the previous one.

Example

This example shows how to configure the trust-point “TP1” as the primary trust-point.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

67-6 show crypto pki trustpoints

This command is used to display the trust-points that are configured in the Switch.

show crypto pki trustpoints [*TRUSTPOINT***]**

Parameters

TRUSTPOINT	(Optional) Specifies the name of the trust-point to be displayed.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all trust-points will be displayed.

Example

This example shows how to display all trust-points.

```
Switch# show crypto pki trustpoints

Trustpoint Name        : TP1 (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Trustpoint Name        : TP2
  Imported certificates:
    CA                 : chunagtel.ca
    local certificate  : openflow.crt
local private key  : openflow.prv

Switch#
```

67-7 show ssl-service-policy

This command is used to display the SSL service policy.

show ssl-service-policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the SSL service policy.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

If no parameter is specified, all SSL service policies will be displayed.

Example

This example shows how to display all SSL service policies.

```
Switch# show ssl-service-policy

SSL Policy Name        : policyForHttp
  Enabled Versions :
        TLS 1.0
        TLS 1.1
        TLS 1.2
  Enabled CipherSuites :
        DHE_DSS_WITH_3DES_EDE_CBC_SHA,
        RSA_WITH_3DES_EDE_CBC_SHA,
        RSA_WITH_RC4_128_SHA,
        RSA_WITH_RC4_128_MD5,
        RSA_EXPORT_WITH_RC4_40_MD5
        RSA_WITH_AES_128_CBC_SHA
        RSA_WITH_AES_256_CBC_SHA
        RSA_WITH_AES_128_CBC_SHA256
        RSA_WITH_AES_256_CBC_SHA256
        DHE_DSS_WITH_AES_256_CBC_SHA
        DHE_RSA_WITH_AES_256_CBC_SHA
  Session Cache Timeout: 600
  Secure Trustpoint    : ggg

SSL Policy Name        : policyForFTP
  Enabled Versions :
        TLS 1.0
        TLS 1.1
        TLS 1.2
  Enabled CipherSuites :
        RSA_WITH_RC4_128_MD5,
        RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 1200
  Secure Trustpoint    : domain2

Switch#
```

67-8 ssl-service-policy

This command is used to configure the SSL service policy. Use the **no** form of this command to remove the SSL service policy.

ssl-service-policy *POLICY-NAME* **[version [***VERSION***] | ciphersuite [***CIPHERSUITE***] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

no ssl-service-policy *POLICY-NAME* **[version [***VERSION***] | ciphersuite [***CIPHERSUITE***] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

Parameters

POLICY-NAME	Specifies the name of the SSL service policy.
version *VERSION*	(Optional) Specifies the TLS version. One of the following keywords can be used: • **tls1.0** - Specifies to use TLS version 1.0 as the SSL service policy. • **tls1.1** - Specifies to use TLS version 1.1 as the SSL service policy.

	• **tls1.2** - Specifies to use TLS version 1.2 as the SSL service policy.
ciphersuite *CIPHERSUITE*	(Optional) Specifies the cipher suites that should be used by the secure service when negotiating a connection with a remote peer. When the cipher suite is not configured, the SSL client and server will negotiate the best cipher suite that they both support from the list of available cipher suites. Multiple cipher suites can be specified to be used. Use the no form of this command to disable the selected cipher suites. The following keywords can be used: • **dhe-dss-3des-ede-cbc-sha** - Specifies to use DH key exchange with 3DES-EDE-CBC encryption and SHA for message digest. • **rsa-3des-ede-cbc-sha** - Specifies to use RSA key exchange with 3DES and DES-EDE3-CBC for message encryption and the Secure Hash Algorithm (SHA) for message digest. • **rsa-rc4-128-sha** - Specifies to use RSA key exchange with RC4 128-bit encryption for message encryption and SHA for message digest. • **rsa-rc4-128-md5** - Specifies to use RSA key exchange with RC4 128-bit encryption for message encryption and Message Digest 5 (MD5) for message digest. • **rsa-export-rc4-40-md5** - Specifies to use RSA EXPORT key exchange with RC4 40 bits for message encryption and MD5 for message digest. • **rsa-aes-128-cbc-sha** - Specifies to use RSA key exchange with AES 128-bit encryption for message encryption and SHA for message digest. • **rsa-aes-256-cbc-sha** - Specifies to use RSA key exchange with AES 256-bit encryption for message encryption and SHA for message digest. • **rsa-aes-128-cbc-sha256** - Specifies to use RSA key exchange with AES 128-bit encryption for message encryption and SHA 256-bit for message digest. • **rsa-aes-256-cbc-sha256** - Specifies to use RSA key exchange with AES 256-bit encryption for message encryption and SHA 256-bit for message digest. • **dhe-dss-aes-256-cbc-sha** - Specifies to use DH key exchange with AES 256-bit encryption and SHA for message digest. • **dhe-rsa-aes-256-cbc-sha** - Specifies to use DH key exchange with AES 256-bit encryption and SHA for message digest.
secure-trustpoint *TRUSTPOINT*	(Optional) Specifies the name of the trust-point that should be used in SSL handshake. When this parameter is not specified, the trust-point which is specified as the primary will be used. If no primary trust-point is specified, the built-in certificate/key pairs will be used. In no form of this command, the specified trust-point will be canceled and then the built-in certificate/key pairs will be used.
session-cache-timeout *TIME-OUT*	(Optional) Specifies the timeout value in seconds for the information stored in the SSL session cache. The valid range is from 60 to 86400. When this parameter is not configured, the default session cache timeout is 600 seconds. In the no form of this command, the SSL session cache timeout will be reverted to the default value.

Default

None.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the SSL service policy.

Example

This example shows how to configure the SSL service policy “ssl-server” which associates the “TP1” trust-point.

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

67-9 crypto pki certificate generate

This command is used to generate a new self-signed certificate.

crypto pki certificate generate

Parameters

None.

Default

By default, the Switch automatically generates a random build-in certificate.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to generate a new self-signed certificate regardless there is a build-in self-signed certificate or not. The Switch will generate a new self-signed certificate automatically if no certificate is detected after the Switch booted up.

The certificate generated by this command does not affect the user-downloaded certificates.

NOTE: This command only supports self-signature RSA certificate with the key length of 2048.

Example

This example shows how to generate a new self-signed certificate.

```
Switch# configure terminal
Switch(config)# crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

68. Virtual LAN (VLAN) Commands

68-1 acceptable-frame

This command is used to set the acceptable types of frames by a port. Use the **no** form of this command to revert to the default settings.

acceptable-frame {tagged-only | untagged-only | admit-all}

no acceptable-frame

Parameters

tagged-only	Specifies that only tagged frames are admitted.
untagged-only	Specifies that only untagged frames are admitted.
admit-all	Specifies that all frames are admitted.

Default

For the access VLAN mode, the default option is untagged-only.

For the other VLAN mode, the default option is admit-all.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to set the acceptable types of frames by a port.

Example

This example shows how to set the acceptable frame type to **tagged-only** on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

68-2 ingress-checking

This command is used to enable ingress checking for frames received by a port. Use the **no** form of this command to disable the ingress check.

ingress-checking

no ingress-checking

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to enable ingress checking for packets received by the interface. If ingress checking is enabled, the packet will be dropped if the received port is not a member port of the VLAN classified for the received packet.

Example

This example shows how to enable ingress checking on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ingress-checking
Switch(config-if)#
```

68-3 show vlan

This command is used to display the parameters for all configured VLANs or one VLAN on the Switch.

show vlan [*VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]]]**

Parameters

VLAN-ID	(Optional) Specifies a list of VLANs to display the member port information. If the VLAN is not specified, all VLANs are displayed. The valid range is from 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the port to display the VLAN related setting.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the parameters for all configured VLANs or one VLAN on the Switch.

Example

This example shows how to display all the current VLAN entries.

```
Switch#show vlan

 VLAN 1
   Name : default
   Description :
   Tagged Member Ports   :
   Untagged Member Ports : eth1/0/1-1/0/28

 Total Entries : 1

Switch#
```

This example shows how to display the PVID, ingress checking, and acceptable frame type information for ports 1 to 2.

```
Switch#show vlan interface eth1/0/1-2

 eth1/0/1
   VLAN Mode             : Hybrid
   Native VLAN           : 1
   Hybrid Untagged VLAN  : 1
   Hybrid Tagged VLAN    :
   Ingress Checking      : Enabled
   Acceptable Frame Type : Admit-All

 eth1/0/2
   VLAN Mode             : Hybrid
   Native VLAN           : 1
   Hybrid Untagged VLAN  : 1
   Hybrid Tagged VLAN    :
   Ingress Checking      : Enabled
   Acceptable Frame Type : Admit-All


Switch#
```

68-4 switchport access vlan

This command is used to specify the access VLAN for an interface. Use the **no** form of this command to revert to the default setting.

switchport access vlan *VLAN-ID*

no switchport access vlan

Parameters

VLAN-ID	Specifies the access VLAN of the interface.

Default

By default, this access VLAN is VLAN 1.

Command Mode

Interface Configuration Mode.

Usage Guideline

The command takes effect when the interface is set to access mode. The VLAN specified as the access VLAN does not need to exist to configure the command.

Only one access VLAN can be specified. The succeeding command overwrites the previous command.

Example

This example shows how to configure port 1 to access mode with access VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1000
Switch(config-if)#
```

68-5 switchport hybrid allowed vlan

This command is used to specify the tagged or untagged VLANs for a hybrid port. Use the **no** form of this command to revert to the default setting.

switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* **[, | -]**

no switchport hybrid allowed vlan

Parameters

add	(Optional) Specifies the port will be added into the specified VLAN(s).
remove	Specifies the port will be removed from the specified VLAN(s).
tagged	Specifies the port as a tagged member of the specified VLAN(s).
untagged	Specifies the port as an untagged member of the specified VLAN(s).
VLAN-ID	Specified the allowed VLAN list or the VLAN list to be added to or removed from the allow VLAN list. If no option is specified, the specified VLAN list will overwrite the allowed VLAN list.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, a hybrid port is an untagged member port of VLAN 1.

Command Mode

Interface Configuration Mode.

Usage Guideline

By setting the hybrid VLAN command multiple times with different VLAN IDs, a port can be a tagged member port or an untagged member port of multiple VLANs.

When the allowed VLAN is only specified as the VLAN ID, the succeeding command will overwrites the previous command. If the new untagged allowed VLAN list is overlap with the current tagged allowed VLAN list, the overlap part will change to the untagged allowed VLAN. On the other hand, if the new tagged allowed VLAN list is overlap with current untagged allowed VLAN list, the overlap part will change to the tagged allowed VLAN. The last command will take effect. The VLAN does not need to exist to configure the command.

Example

This example shows how to configure port 1 to be a tagged member of VLAN 1000 and an untagged member of VLAN 2000 and 3000.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add tagged 1000
Switch(config-if)# switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

68-6 switchport hybrid native vlan

This command is used to specify the native VLAN ID of a hybrid port. Use the **no** form of this command to revert to the default setting.

switchport hybrid native vlan *VLAN-ID*

no switchport hybrid native vlan

Parameters

VLAN-ID	Specifies the native VLAN of a hybrid port.

Default

By default, the native VLAN of a hybrid port is VLAN 1.

Command Mode

Interface Configuration Mode.

Usage Guideline

When configuring the hybrid port join to its native VLAN, use the **switchport hybrid allowed vlan** command to add the native VLAN into its allowed VLAN. The specified VLAN does not need to exist to apply the command. The command takes effect when the interface is set to hybrid mode.

Example

This example shows how to configure port 1 to become a hybrid interface and configure the PVID to 20.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode hybrid
Switch(config-if)# switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)# switchport hybrid native vlan 20
Switch(config-if)#
```

68-7 switchport mode

This command is used to specify the VLAN mode for the port. Use the **no** form of this command to revert to the default setting.

switchport mode {access | hybrid | trunk}

no switchport mode

Parameters

access	Specifies the port as an access port.
hybrid	Specifies the port as a hybrid port.
trunk	Specifies the port as a trunk port.

Default

By default, this option is hybrid.

Command Mode

Interface Configuration Mode.

Usage Guideline

When a port is set to access mode, this port will be an untagged member of the access VLAN configured for the port. When a port is set to hybrid mode, the port can be an untagged or tagged member of any VLAN configured.

When a port is set to trunk mode, this port is either a tagged or untagged member port of its native VLAN and can be a tagged member of other VLANs configured. The purpose of a trunk port is to support the switch-to-switch connection.

When the switch-port mode is changed, the VLAN related setting associated with previous mode will be lost.

Example

This example shows how to configure port 1 as a trunk port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

68-8 switchport trunk allowed vlan

This command is used to configure the VLANs that are allowed to receive and send traffic on the specified interface in a tagged format. Use the **no** form of this command to revert to the default setting.

switchport trunk allowed vlan {all | [add | remove | except] *VLAN-ID* **[, | -]}**

no switchport trunk allowed vlan

Parameters

all	Specifies that all VLANs are allowed on the interface.
add	(Optional) Specifies to add the specified VLAN list to the allowed VLAN list.
remove	(Optional) Specifies to remove the specified VLAN list from the allowed VLAN list.

except	(Optional) Specifies that all VLANs except the VLANs in the exception list are allowed.
VLAN-ID	Specifies the allow VLAN list or the VLAN list to be added to or removed from the allow VLAN list.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, all VLANs are allowed.

Command Mode

Interface Configuration Mode.

Usage Guideline

This command only takes effect when the interface is set to trunk mode. If a VLAN is allowed on a trunk port, the port will become the tagged member of the VLAN. When the allowed VLAN option is set to **all**, the port will be automatically added to all the VLAN created by the system.

Example

This example shows how to configure port 1 as a tagged member of VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan add 1000
Switch(config-if)#
```

68-9 switchport trunk native vlan

This command is used to specify the native VLAN ID of a trunk mode interface. Use the **no** form of this command to revert to the default setting.

switchport trunk native vlan {*VLAN-ID* **| tag}**

no switchport trunk native vlan [tag]

Parameters

VLAN-ID	Specifies the native VLAN for a trunk port.
tag	Specifies to enable the tagging mode of the native VLAN.

Default

By default, the native VLAN is 1, untagged mode.

Command Mode

Interface Configuration Mode.

Usage Guideline

The command only takes effect when the interface is set to trunk mode. When a trunk port native VLAN is set to tagged mode, normally the acceptable frame type of the port should be set to “tagged-only” to only accept tagged frames. When a trunk port works in the untagged mode for a native VLAN, transmitting untagged packet for a native VLAN and tagged packets for all other VLANs and the acceptable frame types of the port has to be set to “admit-all” in order to function correctly.

The specified VLAN does not need to exist to apply the command.

Example

This example shows how to configure port 1 as a trunk interface and configures the native VLAN to 20.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk native vlan 20
Switch(config-if)#
```

68-10 vlan

This command is used to add VLANs and enter the VLAN configuration mode. Use the **no** form of this command to remove VLANs.

vlan *VLAN-ID* **[, | -]**

no vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the ID of the VLAN to be added, removed or configured. The valid VLAN ID range is from 1 to 4094. VLAN ID 1 cannot be removed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

The VLAN ID 1 exists in the system as the default VLAN.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to create VLANs. Entering the **vlan** command with a VLAN ID enters the VLAN Configuration Mode. Entering the VLAN ID of an existing VLAN does not create a new VLAN, but allows the user to modify the VLAN parameters for the specified VLAN. When the user enters the VLAN ID of a new VLAN, the VLAN will be automatically created.

Use the **no vlan** command to remove a VLAN. The default VLAN cannot be removed. If the removed VLAN is a port’s access VLAN, the port’s access VLAN will be reset to VLAN 1.

Example

This example shows how to add new VLANs, assigning the new VLANs with the VLAN IDs 1000 to 1005.

```
Switch#configure terminal
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

68-11 name

This command is used to specify the name of a VLAN. Use the **no** form of this command to revert to the default setting.

name *VLAN-NAME*

no name

Parameters

VLAN-NAME	Specifies the VLAN name, with a maximum of 32 characters. The VLAN name must be unique within the administrative domain.

Default

The default VLAN name is VLANx, where x represents four numeric digits (including the leading zeros) that are equal to the VLAN ID.

Command Mode

VLAN Configuration Mode.

Usage Guideline

Use this command to specify the name of a VLAN. The VLAN name must be unique within the administrative domain.

Example

This example shows how to configure the VLAN name of VLAN 1000 to be “admin-vlan”.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# name admin-vlan
Switch(config-vlan)#
```

69. Voice VLAN Commands

69-1 voice vlan

This command is used to enable the global voice VLAN state and configure the voice VLAN. Use the **no** form of this command to disable the voice VLAN state.

voice vlan *VLAN-ID*

no voice vlan

Parameters

VLAN-ID	Specifies the ID of the voice VLAN. The valid range is from 2 to 4094.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to enable the global voice VLAN function and to specify the voice VLAN on a switch. The switch has only one voice VLAN.

Both the **voice vlan** command in the Global Configuration Mode and the **voice vlan enable** command in the Interface Configuration Mode need to be enabled for a port to start the voice VLAN function.

When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets comply with the OUI addresses configured by the **voice vlan mac-address** command.

The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. If the voice VLAN is configured, then the voice VLAN cannot be removed with the **no vlan** command.

Example

This example shows how to enable the voice VLAN function and configure VLAN 1000 as the voice VLAN.

```
Switch# configure terminal
Switch(config)# voice vlan 1000
Switch(config)#
```

69-2 voice vlan aging

This command is used to configure the aging time for aging out the voice VLAN's dynamic member ports. Use the **no** form of this command to revert to the default setting.

voice vlan aging *MINUTES*

no voice vlan aging

Parameters

MINUTES	Specifies the aging time of the voice VLAN. The valid range is from 1 to 65535 minutes.

Default

By default, this value is 720 minutes.

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to configure the aging time for aging out the voice device and the voice VLAN automatically learned member ports. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled.

Example

This example shows how to configure the aging time of the voice VLAN to 30 minutes.

```
Switch# configure terminal
Switch(config)# voice vlan aging 30
Switch(config)#
```

69-3 voice vlan enable

This command is used to enable the voice VLAN state of ports. Use the **no** form of this command to disable the voice VLAN's port state.

voice vlan enable

no voice vlan enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Usage Guideline

U The command takes effect for access ports or hybrid ports. Use the **voice vlan enable** command to enable the voice VLAN function for ports. oth the **voice vlan** command in the Global Configuration Mode and the **voice vlan enable** command in the Interface Configuration Mode need to be enabled for a port to start the voice VLAN function.

Example

This example shows how to enable the voice VLAN function on port 1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# voice vlan enable
Switch(config-if)#
```

69-4 voice vlan mac-address

This command is used to add the user-defined voice device OUI. Use the **no** form of this command to delete the user-defined voice device OUI.

voice vlan mac-address *MAC-ADDRESS MASK* **[description** *TEXT***]**

no voice vlan mac-address *MAC-ADDRESS MASK*

Parameters

MAC-ADDRES	Specifies the OUI MAC address.
MASK	Specifies the OUI MAC address matching bitmask.
description *TEXT*	(Optional) Specifies the description for the user defined OUI with a maximum of 32 characters.

Default

The default OUI is listed in the following table:

OUI	Vendor
00:E0:BB	3COM
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/Philips
00:0F:E2	Huawei-3COM
00:09:6E	Avaya

Command Mode

Global Configuration Mode.

Usage Guideline

Use this command to add a user-defined OUI for the voice VLAN. The OUI for the voice VLAN is used to identify the voice traffic by using the voice VLAN function. If the source MAC addresses of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet.

The user-defined OUI cannot be the same as the default OUI. The default OUI cannot be deleted.

Example

This example shows how to add a user-defined OUI for voice devices.

```
Switch# configure terminal
Switch(config)# voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

69-5 voice vlan mode

This command is used to enable the automatic learning of the port as voice VLAN member ports. Use the **no** form of this command to disable the automatic learning.

voice vlan mode {manual | auto {tag | untag}}

no voice vlan mode

Parameters

manual	Specifies that voice VLAN membership will be manually configured.
auto	Specifies that voice VLAN membership will be automatically learned.
tag	Specifies to learn voice VLAN tagged members.
untag	Specifies to learn voice VLAN untagged members.

Default

By default, this option is set to untag and auto.

Command Mode

Interface Configuration Mode.

Usage Guideline

Use this command to configure automatic learning or manual configuration of voice VLAN member ports.

If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will be automatically be aged out. When the port is working in the **auto tagged** mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the switch will change its priority. When the voice device sends untagged packets, it will forward them in port's PVID VLAN.

When the port is working in **auto untagged** mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the switch will change its priority. When the voice device sends untagged packets, it will forward them in voice VLAN.

When the switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The switch should follow the tagged flag and priority setting.

If auto learning is disabled, the user should use the **switchport hybrid vlan** command to configure the port as a voice VLAN tagged or untagged member port.

Example

This example shows how to configure port 1 to be in the **auto tag** mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# voice vlan mode auto tag
Switch(config-if)#
```

69-6 voice vlan qos

This command is used to configure the CoS priority for the incoming voice VLAN traffic. Use the **no** form of this command to revert to the default setting.

voice vlan qos *COS-VALUE*

no voice vlan qos

Parameters

COS-VALUE	Specifies the priority of the voice VLAN. This value must be between 0 and 7.

Default

By default, this value is 5.

Command Mode

Global Configuration Mode.

Usage Guideline

The voice packets arriving at the voice VLAN enabled port are marked to the CoS specified by the command. The remarking of CoS allows the voice VLAN traffic to be distinguished from data traffic in quality of service.

Example

This example shows how to configure the priority of the voice VLAN to be 7.

```
Switch# configure terminal
Switch(config)# voice vlan qos 7
Switch(config)#
```

69-7 show voice vlan

This command is used to display the voice VLAN configuration.

show voice vlan [interface [*INTERFACE-ID* **[, | -]]]**

show voice vlan {device | lldp-med device} [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface	(Optional) Specifies to display voice VLAN information of ports.
INTERFACE-ID	(Optional) Specifies the interface to display.

,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
device	Specifies to display the voice devices learned by OUI.
lldp-med device	Specifies to display the voice devices learned by LLDP-MED.

Default

None.

Command Mode

EXEC Mode.

Usage Guideline

Use this command to display the voice VLAN configuration.

Example

This example shows how to display the voice VLAN global settings.

```
Switch#show voice vlan

 Voice VLAN ID         : 1000
 Voice VLAN CoS        : 7
 Aging Time             : 30 minutes
 Member Ports           : eth1/0/1-1/0/5
 Dynamic Member Ports : eth1/0/1-1/0/3
 Voice VLAN OUI:

 OUI Address        Mask               Description
 ----------------   -----------------   -------------
 00-01-E3-00-00-00  FF-FF-FF-00-00-00    Siemens
 00-03-6B-00-00-00  FF-FF-FF-00-00-00    Cisco
 00-09-6E-00-00-00  FF-FF-FF-00-00-00    Avaya
 00-0F-E2-00-00-00  FF-FF-FF-00-00-00    Huawei&3COM
 00-60-B9-00-00-00  FF-FF-FF-00-00-00    NEC&Philips
 00-D0-1E-00-00-00  FF-FF-FF-00-00-00    Pingtel
 00-E0-75-00-00-00  FF-FF-FF-00-00-00    Veritel
 00-E0-BB-00-00-00  FF-FF-FF-00-00-00    3COM
 00-02-03-00-00-00  FF-FF-FF-00-00-00    User1

 Total OUI: 9

Switch#
```

This example shows how to display the voice VLAN information of ports.

```
Switch#show voice vlan interface eth1/0/1-5

Interface     State       Mode
------------  ----------  ------------
eth1/0/1      Enabled     Auto/Tag
eth1/0/2      Enabled     Manual
eth1/0/3      Enabled     Manual
eth1/0/4      Enabled     Auto/Untag
eth1/0/5      Disabled    Manual

Switch#
```

This example shows how to display the learned voice devices on ports 1 to 2.

```
Switch# show voice vlan device interface eth1/0/1-2

Interface  Device Address     Start Time         Status
---------  ------------------ -----------------  -------
eth1/0/1   00-03-6B-00-00-01  2012-03-19 09:00   Active
eth1/0/1   00-03-6B-00-00-02  2012-03-20 10:09   Aging
eth1/0/1   00-03-6B-00-00-05  2012-03-20 12:04   Active
eth1/0/2   00-03-6B-00-00-0a  2012-03-19 08:11   Aging
eth1/0/2   33-00-61-10-00-11  2012-03-20 06:45   Aging

Total Entries: 5

Switch#
```

This example shows how to display the learned LLDP-MED voice devices on ports 1 to 2.

```
Switch# show voice vlan lldp-med device interface eth1/0/1-2

Index                 : 1
Interface            : eth1/0/1
Chassis ID Subtype : MAC Address
Chassis ID           : 00-E0-BB-00-00-11
Port ID Subtype     : Network Address
Port ID               : 172.18.1.1
Create Time          : 2012-03-19 10:00
Remain Time          : 108 Seconds

Index                 : 2
Interface            : eth1/0/2
Chassis ID Subtype : MAC Address
Chassis ID           : 00-E0-BB-00-00-12
Port ID Subtype     : Network Address
Port ID               : 172.18.1.2
Create Time          : 2012-03-20 11:00
Remain Time          : 105 Seconds

Total Entries: 2

Switch#
```

Appendix A - System Log Entries

The System Log entries are listed in this appendix.

802.1X

Log	Description	Severity
1	Event Description: This log is recorded when IEEE 802.1X authentication failed. Log Message: 802.1X authentication fail [due to <reason>] from (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: reason: The reason for the failed authentication. The possible reason may be: (1) user authentication failure (2) no server(s) responding (3) no servers configured (4) no resources (5) user timeout expired username: The user being authenticated. interface-id: The switch interface number. mac-address: The MAC address of the authenticated device.	Critical
2	Event Description: This log is recorded when IEEE 802.1X authentication is successful. Log Message: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters Description: username: The user being authenticated. interface-id: The interface name. mac-address: The MAC address of the authenticated device.	Informational

AAA

Log	Description	Severity
1	Event Description: This log is recorded when the AAA global state is enabled or disabled. Log Message: AAA is <status> Parameters Description: status: The AAA status.	Informational
2	Event Description: This log is recorded when login is successful. Log Message: Successful login through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL). client-ip: The IP address of the client if valid through IP protocol. aaa-method: The authentication method, for example, none, local, or server. server-ip: The IP address of the AAA server if the authentication method is remote server. username: The username for authentication.	Informational
3	Event Description: This log is recorded when the login failed. Log Message: Login failed through <exec-type> [from <client-ip>] authenticated by AAA <aaa-method> <server-ip> (Username: <username>) Parameters Description: exec-type: The EXEC types, for example, Console, Telnet, SSH, Web, or Web (SSL).	Warning

	client-ip: The IP address of the client if valid through IP protocol. aaa-method: The authentication method, for example, local or server. server-ip: The IP address of the AAA server if the authentication method is remote server. username: The username for authentication.	
4	Event Description: This log is recorded when RADIUS assigned valid VLAN ID attributes. Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) Parameters Description: server-ip: The IP address of the RADIUS server. vid: The assign VLAN ID authorized by the RADIUS server. interface–id: The port number of the authenticated client. username: The username for authentication.	Informational

ARP

Log	Description	Severity
1	Event Description: This log is recorded when gratuitous ARP detected a duplicate IP address. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <port-num>, Interface: <ipif-name>) Parameters Description: ipaddr: The duplicated IP address. macaddr: The MAC address of the duplicated IP address. port-num: The port number of the device. ipif-name: The name of the interface on the switch that contains the duplicated IP address.	Warning

Auto Image

Log	Description	Severity
1	Event Description: This log is recorded when the auto-image firmware upgraded successfully. Log Message: The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: The IP address of the TFTP server.	Informational
2	Event Description: This log is recorded when the auto-image firmware failed to upgrade. Log Message: The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: The IP address of the TFTP server.	Informational

Auto Save Config

Log	Description	Severity
1	Event Description: This log is recorded when the DDP configuration is saved automatically. Log Message:CONFIG-6-DDPSAVECONFIG: Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational

Auto Surveillance VLAN

Log	Description	Severity
1	Event Description: This log is recorded when a new surveillance device is detected on an interface. Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: The name of the interface. mac-address: The MAC address of the surveillance device.	Informational
2	Event Description: This log is recorded when an interface, which is an enabled surveillance VLAN, joins the surveillance VLAN automatically. Log Message: <interface-id> add into surveillance VLAN <vid> Parameters Description: interface-id: The name of the interface. vid: The VLAN ID.	Informational
3	Event Description: This log is recorded when an interface leaves the surveillance VLAN and at the same time no surveillance device is detected in the aging interval for that interface. Log Message: <interface-id> remove from surveillance VLAN <vid> Parameters Description: interface-id: The name of the interface. vid: The VLAN ID.	Informational
4	Event Description: This log is recorded when an IPC is added in the surveillance VLAN. Log Message: ASV: Add IPC (<ipaddr>, MAC:<mac-address>) Parameters Description: ipaddr: The IP address of the IPC. mac-address: The MAC address of the IPC.	Informational
5	Event Description: This log is recorded when an IPC is removed from the surveillance VLAN. Log Message: ASV: Remove IPC (<ipaddr>, MAC:<mac-address>) Parameters Description: ipaddr: The IP address of the IPC. mac-address: The MAC address of the IPC.	Informational
6	Event Description: This log is recorded when an NVR is added in the surveillance VLAN. Log Message: ASV: Add NVR (<ipaddr>, MAC:<mac-address>) Parameters Description: ipaddr: The IP address of the NVR. mac-address: The MAC address of the NVR.	Informational
7	Event Description: This log is recorded when an NVR is removed from the surveillance VLAN. Log Message: ASV: Remove NVR (<ipaddr>, MAC:<mac-address>) Parameters Description: ipaddr: The IP address of the NVR. mac-address: The MAC address of the NVR.	Informational
8	Event Description: This log is recorded when the mode of ASV 2.0 is changed through the Web. Log Message: ASV: Mode change from <mode> to <mode > Parameters Description: mode: The mode of ASV 2.0. This can be standard or surveillance.	Informational

Configuration /Firmware

Log	Description	Severity
1	Event Description: This log is recorded when the firmware was upgraded successfully. Log Message: Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
2	Event Description: This log is recorded when the firmware upgrade failed. Log Message: Firmware upgraded by <session> unsuccessfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
3	Event Description: This log is recorded when the firmware uploaded successfully. Log Message: Firmware uploaded by <session> successfully (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
4	Event Description: This log is recorded when the firmware upload failed. Log Message: Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
5	Event Description: This log is recorded when the configuration downloaded successfully. Log Message: Configuration downloaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server.	Informational

	pathfile: The path and file name on the server.	
6	Event Description: This log is recorded when the configuration download failed. Log Message: Configuration downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
7	Event Description: This log is recorded when the configuration uploaded successfully. Log Message: Configuration uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Informational
8	Event Description: This log is recorded when the configuration upload failed. Log Message: Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning
9	Event Description: This log is recorded when the configuration is saved to the flash through the console. Log Message: Configuration saved to flash by console (Username: <username>) Parameters Description: username: The current login user.	Informational
10	Event Description: This log is recorded when the configuration is saved to the flash remotely. Log Message: Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
11	Event Description: This log is recorded when a log message is uploaded successfully. Log Message: Log message uploaded by <session> successfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client.	Informational
12	Event Description: This log is recorded when a log message upload failed.	Warning

	Log Message: Log message uploaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client.	
13	Event Description: This log is recorded when an unknown type file download failed. Log Message: Downloaded by <session> unsuccessfully. (Username: <username> [, IP: <ipaddr>, MAC: <macaddr>], Server IP: <server-ip>, File Name: <pathfile>) Parameters Description: session: The user's session. username: The current login user. ipaddr: The IP address of the client. macaddr: The MAC address of the client. server-ip: The IP address of the server. pathfile: The path and file name on the server.	Warning

NOTE:

- The user's session indicates Console, Web, SNMP, Telnet, or SSH.
- If the configuration/firmware is updated through the Console, there will be no IP and MAC information for logging.

DAD

Log	Description	Severity
1	Event Description: This log is recorded when the DUT receives a Neighbor Solicitation (NS) message with a duplicate address in the DAD duration, the DUT will add this log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages Parameters Description: ipv6address: The IPv6 address in NS messages interface-id: The interface name.	Warning
2	Event Description: This log is recorded when the DUT receives a Neighbor Advertisement (NA) message with a duplicate address in the DAD duration, the DUT will add this log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages Parameters Description: ipv6address: The IPv6 address in NA messages. interface-id: The interface name.	Warning

DAI

Log	Description	Severity
1	Event Description: This log is recorded when DAI detects invalid ARP packets. Log Message: Illegal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) Parameters Description: type: The type of ARP packet. It indicates an ARP packet request or response. ip-address: The IP address.	Warning

	mac-address: The MAC address. vlan-id: The VLAN ID. interface-id: The name of the interface.	
2	Event Description: This log is recorded when DAI detects valid ARP packets. Log Message: Legal ARP <type> packets (IP: <ip-address>, MAC: <mac-address>, VLAN <vlan-id>, on <interface-id>) Parameters Description: type: The type of ARP packet. It indicates an ARP packet request or response. ip-address: The IP address. mac-address: The MAC address. vlan-id: The VLAN ID. interface-id: The name of the interface.	Informational

DHCPv6 Client

Log	Description	Severity
1	Event Description: This log is recorded when the DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled] Parameters Description: ipif-name: The name of the DHCPv6 client interface.	Informational
2	Event Description: This log is recorded when the DHCPv6 client obtains an IPv6 address from a DHCPv6 server. Log Message: DHCPv6 client obtains an IPv6 address <ipv6address> on interface <ipif-name> Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
3	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, starts renewing. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts renewing Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
4	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, renews success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> renews success Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
5	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, starts rebinding. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> starts rebinding Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational
6	Event Description: This log is recorded when the IPv6 address, obtained from a DHCPv6 server, rebinds success. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> rebinds success Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational

7	Event Description: This log is recorded when the IPv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address <ipv6address> on interface <ipif-name> was deleted Parameters Description: ipv6address: The IPv6 address obtained from a DHCPv6 server. ipif-name: The name of the DHCPv6 client interface.	Informational

DHCPv6 Relay

Log	Description	Severity
1	Event Description: This log is recorded when the DHCPv6 relay on the specified interface's administrator state changed. Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Parameters Description: <ipif-name>: The name of the DHCPv6 relay agent interface.	Informational

DNS Resolver

Log	Description	Severity
1	Event Description: This log is recorded when a duplicate domain name is added to the cache and this leads to the deletion of the dynamic domain name cache. Log Message: Duplicate Domain name case name: <domain-name>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domain-name: The domain name string. ipaddr: The static/dynamic IP address.	Informational

DoS Prevention

Log	Description	Severity
1	Event Description: This log is recorded when a DoS attack is detected. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>) Parameters Description: dos-type: The DoS attack type. ip-address: The IP address. interface-id: The name of the interface.	Notification

Interface

Log	Description	Severity
1	Event Description: This log is recorded when the port link is down. Log Message: Port <port-type><interface-id> link down Parameters Description: port-type: The port type. interface-id: The interface name.	Informational
2	Event Description: This log is recorded when the port link is up. Log Message: Port <port-type><interface-id> link up, <link-speed> Parameters Description:	Informational

port-type: The port type.
interface-id: The interface name.
link-speed: The port link speed.

IPSG

	Log Description	Severity
1	Event Description: This log is recorded when there are no hardware rule resources to set the DHCP snooping entry into the IPSG table. Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlanid>, Interface <interface-id>) Parameters Description: ipaddr: The IP address. macaddr: The MAC address. vlanid: The VLAN ID. interface-id: The interface name.	Warning

IPv6SG

	Log Description	Severity
1	Event Description: This log is recorded when there are no hardware rule resources to set the IPv6 snooping entry into the IPv6SG table. Log Message: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <ipaddr>, MAC: <macaddr>, VID: <vlan-id>, Interface <interface-id>) Parameters Description: ipaddr: The IPv6 address of the IPv6 snooping entry. macaddr: The MAC address of the IPv6 snooping entry. vlan-id: The VLAN ID of the IPv6 snooping entry. interface-id: The interface of the IPv6 snooping entry.	Warning

LACP

	Log Description	Severity
1	Event Description: This log is recorded when the link aggregation group link is up. Log Message: Link Aggregation Group <group-id> link up Parameters Description: group-id: The group ID of the link down aggregation group.	Informational
2	Event Description: This log is recorded when the link aggregation group link is down. Log Message: Link Aggregation Group <group-id> link down Parameters Description: group-id: The group ID of the link down aggregation group.	Informational
3	Event Description: This log is recorded when a member port is attached to the link aggregation group. Log Message: <ifname> attach to Link Aggregation Group <group-id> Parameters Description: ifname: The interface name of the port that is attached to the aggregation group. group-id: The group ID of the aggregation group that the port attached to.	Informational
4	Event Description: This log is recorded when a member port is detached from the link aggregation group.	Informational

	Log Message: <ifname> detach from Link Aggregation Group <group-id> Parameters Description: ifname: The interface name of the port that is detached from the aggregation group. group-id: The group ID of the aggregation group that the port detached from.	

LBD

Log	Description	Severity
1	Event Description: This log is recorded when an interface detects a loop. Log Message: <interface-id> LBD loop occurred Parameters Description: interface-id: The interface on which loop is detected.	Critical
2	Event Description: This log is recorded when an interface detects a loop in a VLAN. Log Message: <interface-id> VLAN <vlan-id> LBD loop occurred Parameters Description: interface-id: The interface on which the loop is detected. vlan-id: The VLAN on which the loop is detected.	Critical
3	Event Description: This log is recorded when an interface loop is recovered. Log Message: <interface-id> LBD loop recovered Parameters Description: interface-id: The interface on which the loop is recovered.	Critical
4	Event Description: This log is recorded when an interface loop is recovered in a VLAN. Log Message: <interface-id> VLAN <vlan-id> LBD loop recovered Parameters Description: interface-id: The interface on which the loop is recovered. vlan-id: The VLAN on which the loop is recovered.	Critical
5	Event Description: This log is recorded when the number of VLANs that loop back exceeds the reserved number. Log Message: Loop VLAN numbers overflow	Critical

LLDP/LLDP-MED

Log	Description	Severity
1	Event Description: This log is recorded when an LLDP-MED topology change is detected. Log Message: LLDP-MED topology change detected (on port <portNum>. chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7). portID: The port ID. deviceClass: The LLDP-MED device type.	Notification
2	Event Description: This log is recorded when an LLDP-MED device type conflict is detected. Log Message: Conflict LLDP-MED device type detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) Parameters Description:	Notification

	portNum: The port number. chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7). portID: The port ID. deviceClass: The LLDP-MED device type.	
3	Event Description: This log is recorded when an incompatible LLDP-MED TLV set is detected. Log Message: Incompatible LLDP-MED TLV set detected (on port <portNum>, chassis ID: <chassisType>, <chassisID>, port ID: <portType>, <portID>, device class: <deviceClass>) Parameters Description: portNum: The port number. chassisType: The chassis ID subtype. This can be chassisComponent (1), interfaceAlias (2), portComponent (3), macAddress (4), networkAddress (5), interfaceName (6), or local (7). chassisID: The chassis ID. portType: The port ID subtype. This can be interfaceAlias (1), portComponent (2), macAddress (3), networkAddress (4), interfaceName (5), agentCircuitId (6), or local (7). portID: The port ID. deviceClass: The LLDP-MED device type.	Notification

Login/Logout CLI

Log	Description	Severity
1	Event Description: This log is recorded when login through the console is successful. Log Message: Successful login through Console (Username: <username>) Parameters Description: username: The current login user.	Informational
2	Event Description: This log is recorded when login through the console failed. Log Message: Login failed through Console (Username: <username>) Parameters Description: username: The current login user.	Warning
3	Event Description: This log is recorded when the console session timed out. Log Message: Console session timed out (Username: <username>) Parameters Description: username: The current login user.	Informational
4	Event Description: This log is recorded when logout from the console occurred. Log Message: Logout through Console (Username: <username>) Parameters Description: username: The current login user.	Informational
5	Event Description: This log is recorded when login through Telnet is successful. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
6	Event Description: This log is recorded when login through Telnet failed. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Warning

7	Event Description: This log is recorded when the Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
8	Event Description: This log is recorded when logout from Telnet occurred. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
9	Event Description: This log is recorded when login through SSH is successful. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
10	Event Description: This log is recorded when login through SSH failed. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Critical
11	Event Description: This log is recorded when the SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational
12	Event Description: This log is recorded when logout from SSH occurred. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: The current login user. ipaddr: The IP address of the client.	Informational

MSTP Debug Enhancement

Log	Description	Severity
1	Event Description: This log is recorded when the Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
2	Event Description: This log is recorded when the Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
3	Event Description: This log is recorded when an MSTP instance topology change event occurs. Log Message: Topology changed (Instance: <instance-id>,<interface-id>, MAC:<macaddr>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. macaddr: The MAC address of the bridge.	Notification
4	Event Description: This log is recorded when a new MSTP instance root bridge is selected. Log Message: [CIST | CIST Region | MSTI Region] New Root bridge selected ([Instance: <instance-id>] MAC: <macaddr> Priority:<priority>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.	Informational

	macaddr: The MAC address of the bridge. priority: The bridge priority value. This is divisible by 4096.	
5	Event Description: This log is recorded when a new MSTP instance root port is selected. Log Message: New root port selected (Instance:<instance-id>, <interface-id>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information.	Notification
6	Event Description: This log is recorded when an MSTP instance port state change event occurs. Log Message: Spanning Tree port status change (Instance:<instance-id>, <interface-id>) <old-status> -> <new-status> Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. old-status: The old status of the port. This can be Disable, Discarding, Learning, or Forwarding. new-status: The new status of the port. This can be Disable, Discarding, Learning, or Forwarding.	Notification
7	Event Description: This log is recorded when an MSTP instance port role change event occurs. Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) <old-role> -> <new-role> Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number that detects or receives topology change information. old-role: The old STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort. new-role: The new STP role. This can be DisablePort, AlternatePort, BackupPort, RootPort, DesignatedPort, NonstpPort, or MasterPort.	Informational
8	Event Description: This log is recorded when an MST instance is created. Log Message: Spanning Tree instance created (Instance:<instance-id>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.	Informational
9	Event Description: This log is recorded when an MST instance is deleted. Log Message: Spanning Tree instance deleted (Instance:<instance-id>) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST.	Informational
10	Event Description: This log is recorded when STP version changes. Log Message: Spanning Tree version change (new version:<new-version>) Parameters Description: new-version: The active STP version.	Informational
11	Event Description: This log is recorded when the configuration name and revision level changed in the MST configuration identification. Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name>, revision level <revision-level>) Parameters Description: name: The name given for the specified MST region. revision-level: The revision level. Switches using the same given name but with a different revision level are considered members of different MST regions.	Informational
12	Event Description: This log is recorded when a VLAN is mapped to an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. startvlanid: The starting VLAN ID in the VLAN range to be added.	Informational

	endvlanid: The ending VLAN ID in the VLAN range to be added.	
13	Event Description: This log is recorded when a VLAN is deleted from an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <instance-id> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. startvlanid: The starting VLAN ID in the VLAN range to be deleted. endvlanid: The ending VLAN ID in the VLAN range to be deleted.	Informational
14	Event Description: This log is recorded when the port role changes to alternate due to guard root. Log Message: Spanning Tree port role change (Instance:<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: instance-id: The MST instance ID. Instance 0 represents the default instance, CIST. interface-id: The port number which detects the event.	Informational

Peripheral

Log	Description	Severity
1	Event Description: This log is recorded when the fan is recovered. Log Message: <fan-descr> back to normal Parameters Description: fan-descr: The fan ID and position.	Critical
2	Event Description: This log is recorded when a fan failed. Log Message: <fan-descr> failed Parameters Description: fan-descr: The fan ID and position.	Critical
3	Event Description: This log is recorded when the temperature sensor enters the alarm state. Log Message: <thermal-sensor-descr> detects abnormal temperature <degree> Parameters Description: thermal-sensor-descr: The sensor ID and position. degree: The current temperature.	Critical
4	Event Description: This log is recorded when the temperature recovers to normal. Log Message: <thermal-sensor-descr> temperature back to normal Parameters Description: thermal-sensor-descr: The sensor ID and position.	Critical
5	Event Description: This log is recorded when factory reset button is pressed. Log Message: Factory reset button pressed	Critical

Port Security

Log	Description	Severity
1	Event Description: This log is recorded when a MAC address causes a port security violation. Log Message: MAC address <macaddr> causes port security violation on <interface-id> Parameters Description: macaddr: The violation MAC address. interface-id: The interface name.	Warning
2	Event Description: This log is recorded when the address table is full on the system Log Message: Limit on system entry number has been exceeded	Warning

Safeguard

	Log Description	Severity
1	Event Description: This log is recorded when the host enters the exhausted mode. Log Message: Safeguard Engine enters EXHAUSTED mode	Warning
2	Event Description: This log is recorded when the host enters the normal mode. Log Message: Safeguard Engine enters NORMAL mode	Informational

SNMP

	Log Description	Severity
1	Event Description: This log is recorded when an SNMP request is received with an invalid community string. Log Message: SNMP request received from <ipaddr> with invalid community string Parameters Description: ipaddr: The IP address.	Informational

SSH

	Log Description	Severity
1	Event Description: This log is recorded when the SSH server is enabled. Log Message: SSH server is enabled	Informational
2	Event Description: This log is recorded when the SSH server is disabled. Log Message: SSH server is disabled	Informational

Storm Control

	Log Description	Severity
1	Event Description: This log is recorded when a storm is occurring. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id> Parameters Description: Broadcast: A broadcast storm is occurring. Broadcast packets (DA = FF:FF:FF:FF:FF:FF). Multicast: A multicast storm is occurring. Multicast packets may include unknown L2 multicast, known L2 multicast, unknown IP multicast, and known IP multicast. Unicast: A unicast storm is occurring. Unicast packets may include both known and unknown unicast packets. interface-id: The interface ID on which a storm is occurring.	Warning
2	Event Description: This log is recorded when the storm is cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id> Parameters Description: Broadcast: The broadcast storm is cleared. Multicast: The multicast storm is cleared. Unicast: The unicast storm is cleared. This includes both known and unknown unicast packets. interface-id: The interface ID on which a storm is cleared.	Informational
3	Event Description: This log is recorded when a port is shut down due to a packet storm. Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm	Warning

	Parameters Description: interface-id: The interface ID that was error-disabled because of the storm. Broadcast: The interface is disabled due to a broadcast storm occurrence. Multicast: The interface is disabled due to a multicast storm occurrence. Unicast: The interface is disabled due to a unicast storm occurrence. This includes both known and unknown unicast packets.	

System

Log	Description	Severity
1	Event Description: This log is recorded when the system warm start. Log Message: System warm start	Critical
2	Event Description: This log is recorded when the system cold start. Log Message: System cold start	Critical
3	Event Description: This log is recorded when the system starts up. Log Message: System started up	Critical

Telnet

Log	Description	Severity
1	Event Description: This log is recorded when login through Telnet is successful. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational
2	Event Description: This log is recorded when login through Telnet failed. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Warning
3	Event Description: This log is recorded when logout from Telnet is successful. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of the Telnet client.	Informational
4	Event Description: This log is recorded when the Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the Telnet client. ipaddr: The IP address of Telnet client.	Informational

Voice VLAN

Log	Description	Severity
1	Event Description: This log is recorded when a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: <mac-address>) Parameters Description:	Informational

	interface-id: The interface name. mac-address: The MAC address of the voice device.	
2	Event Description: This log is recorded when an interface, in the auto-voice VLAN mode, joins the voice VLAN. Log Message: <interface-id> add into voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational
3	Event Description: This log is recorded when an interface leaves the voice VLAN and no voice device is detected in the aging interval for that interface. Log Message: <interface-id> remove from voice VLAN <vid> Parameters Description: interface-id: The interface name. vid: The VLAN ID.	Informational

Web

Log	Description	Severity
1	Event Description: This log is recorded when login through the Web is successful. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.	Informational
2	Event Description: This log is recorded when login through the Web failed. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.	Warning
3	Event Description: This log is recorded when the Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.	Informational
4	Event Description: This log is recorded when logout through the Web is successful. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username of the HTTP client. ipaddr: The IP address of the HTTP client.	Informational
5	Event Description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
6	Event Description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
7	Event Description: Web (SSL) session timed out.	Informational

	Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	
8	Event Description: Logout through Web (SSL). Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The username that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Appendix B - Trap Entries

The Trap Log entries are listed in this appendix.

802.1X

Trap	Name	Description	OID
1	dDot1xExtLoggedSuccess	This trap is sent when a host passed IEEE 802.1X authentication (login successful). Binding Objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.171.14.30.0.1
2	dDot1xExtLoggedFail	This trap is sent when a host failed to pass IEEE 802.1X authentication (login failed). Binding Objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.171.14.30.0.2

Authentication Fail

Trap	Name	Description	OID
1	authenticationFailure	This trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of SNMPv2 must be capable to generate this trap, the *snmpEnableAuthenTraps* object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

DHCP Server Screen Prevention

Trap	Name	Description	OID
1	dDhcpFilterAttackDetected	This trap is sent when DHCP server screen is enabled and the switch received a forged DHCP Server packet. Binding Objects: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.171.14.133.0.1

DoS Prevention

Trap	Name	Description	OID
1	dDosPreveAttackDetectedPacket	This trap is sent when a DoS attack is detected.	1.3.6.1.4.1.171.14.59.0.2

		Binding Objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	

ErrDisable

Trap	Name	Description	OID
1	dErrDisNotifyPortDisabledAssert	This trap is sent when a port enters the error-disabled state. Binding Objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.1
2	dErrDisNotifyPortDisabledClear	This trap is sent when a port-loop restarts after the interval time. Binding Objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.171.14.45.0.2

General Management

Trap	Name	Description	OID
1	dGenMgmtLoginFail	This trap is sent when the user login failed to the switch. Binding Objects: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.171.14.165.0.1

Gratuitous ARP

Trap	Name	Description	OID
1	agentGratuitousARPTrap	This trap is sent when an IP address conflict occurred. Binding Objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.171.14.75.0.1

IMPB

Trap	Name	Description	OID
1	dImpbViolationTrap	This trap is sent when the switch detects an IPMB address violation. Binding Objects: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress	1.3.6.1.4.1.171.14.22.0.1

		(5) dImpbViolationVlan	

LACP

Trap	Name	Description	OID
1	linkUp	This trap signifies that the SNMP entity, acting in an agent role, has detected that the *ifOperStatus* object for one of its communication links left the down state and transitioned into another state (not the *notPresent* state). The new state is indicated in *ifOperStatus*. Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	This trap signifies that the SNMP entity, acting in an agent role, has detected that the *ifOperStatus* object for one of its communication links is about to enter the down state from another state (not from the *notPresent* state). This old state is indicated in *ifOperStatus*. Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

LBD

Trap	Name	Description	OID
1	dLbdLoopOccurred	This trap is sent when an interface loop occurs. Binding Objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.1
2	dLbdLoopRestart	This trap is sent when an interface loop restarts after the interval time. Binding Objects: (1) dLbdNotifyInfoIfIndex	1.3.6.1.4.1.171.14.46.0.2
3	dLbdVlanLoopOccurred	This trap is sent when an interface with a VID loop occurs. Binding Objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.3
4	dLbdVlanLoopRestart	This trap is sent when an interface loop with a VID restarts after the interval time. Binding Objects: (1) dLbdNotifyInfoIfIndex (2) dLbdNotifyInfoVlanId	1.3.6.1.4.1.171.14.46.0.4

LLDP/LLDP-MED

Trap	Name	Description	OID
1	lldpRemTablesChange	This trap is sent when the value in *lldpStatsRemTableLastChangeTime* changes.	1.0.8802.1.1.2.0.0.1

		Binding Objects: (1) lldpStatsRemTablesInserts (2) lldpStatsRemTablesDeletes (3) lldpStatsRemTablesDrops (4) lldpStatsRemTablesAgeouts	
2	lldpXMedTopologyChangeDetected	This trap is sent by the local device sensing a change in the topology that indicates a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding Objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1

MAC Notification

Trap	Name	Description	OID
1	swL2macNotification	This trap indicates a MAC address variation in the MAC address table. Binding Objects: (1) swL2macNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
2	dL2FdbMacNotificationWithVID	This trap indicates a MAC address variation in the MAC address table. Binding Objects: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2

MSTP

Trap	Name	Description	OID
1	newRoot	This trap indicates that the sending agent has become the new root of the Spanning Tree. This trap is sent by a bridge after its election as the new root. For example, upon the expiration of the Topology Change Timer or immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
2	topologyChange	This trap is sent by a bridge when any of its configured ports transitions from the *Learning* state to the *Forwarding* state, or from the *Forwarding* state to the *Blocking* state. This trap is not sent if a *newRoot* trap is sent for the same transition. Implementation of this trap is optional	1.3.6.1.2.1.17.0.2

Peripheral

Trap	Name	Description	OID
1	dEntityExtFanStatusChg	This trap is sent from the commander switch when a fan fails (*dEntityExtEnvFanStatus* is 'fault') or recovers (*dEntityExtEnvFanStatus* is 'ok'). Binding Objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex	1.3.6.1.4.1.171.14.5.0.1

		(3) dEntityExtEnvFanStatus	
2	dEntityExtThermalStatusChg	This trap is sent from the commander switch when a thermal alarms (*dEntityExtEnvTempStatus* is 'abnormal') or recovers (*dEntityExtEnvTempStatus* is 'ok'). Binding Objects: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2

Port

Trap	Name	Description	OID
1	linkUp	This trap is generated when the port link status changes to up. Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
2	linkDown	This trap is generated when the port link status changes to down. Binding Objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

Port Security

Trap	Name	Description	OID
1	dPortSecMacAddrViolation	This trap is sent when new MAC addresses violate the pre-defined port security configuration. Binding Objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfLastMacAddress	1.3.6.1.4.1.171.14.8.0.1

RMON

Trap	Name	Description	OID
1	risingAlarm	This trap is sent when an alarm entry crosses its rising threshold and generates an event that is configured for sending SNMP traps. Binding Objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmRisingThreshold	1.3.6.1.2.1.16.0.1

2	fallingAlarm	This trap is sent when an alarm entry crosses its falling threshold and generates an event that is configured for sending SNMP traps. Binding Objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold	1.3.6.1.2.1.16.0.2

Safeguard

Trap	Name	Description	OID
1	dSafeguardChgToExhausted	This trap indicates a change in the system operation mode from normal to exhaust. Binding Objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.1
2	dSafeguardChgToNormal	This trap indicates a change in the system operation mode from exhausted to normal. Binding Objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.171.14.19.1.1.0.2

Start

Trap	Name	Description	OID
1	coldStart	This trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself and that its configuration may have been altered.	1.3.6.1.6.3.1.1.5.1
2	warmStart	This trap signifies that the SNMPv2 entity, acting in an agent role, is reinitializing itself such that its configuration is unaltered.	1.3.6.1.6.3.1.1.5.2

Storm Control

Trap	Name	Description	OID
1	dStormCtrlOccurred	This trap is sent when *dStormCtrlNotifyEnable* is *stormOccurred* or 'both', and a storm is detected. Binding Objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.1
2	dStormCtrlStormCleared	This trap is sent when *dStormCtrlNotifyEnable* is *stormCleared* or 'both', and a storm is cleared. Binding Objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.171.14.25.0.2

System File

Trap	Name	Description	OID
1	dsfUploadImage	This trap is sent when the user uploaded an image file successfully.	1.3.6.1.4.1.171.14.14.0.1
2	dsfDownloadImage	This trap is sent when the user downloaded an image file successfully.	1.3.6.1.4.1.171.14.14.0.2
3	dsfUploadCfg	This trap is sent when the user uploaded a configuration file successfully.	1.3.6.1.4.1.171.14.14.0.3
4	dsfDownloadCfg	This trap is sent when the user downloaded a configuration file successfully.	1.3.6.1.4.1.171.14.14.0.4
5	dsfSaveCfg	This trap is sent when the user saved the configuration file successfully.	1.3.6.1.4.1.171.14.14.0.5

Appendix C - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch is used in the 802.1X module.

The description that follows explains the following RADIUS Attributes Assignment types:

- VLAN

To assign the **VLAN** by the RADIUS server, the proper parameters should be configured on the RADIUS server. To use VLAN assignment, RFC 3580 defines the following tunnel attributes in RADIUS packets.

The table below shows the parameters for a VLAN:

RADIUS Tunnel Attribute	Description	Value	Usage
Tunnel-Type	This attribute indicates the tunneling protocol(s) to be used (in the case of a tunnel initiator) or the tunneling protocol in use (in the case of a tunnel terminator).	13 (VLAN)	Required
Tunnel-Medium-Type	This attribute indicates the transport medium being used.	6 (802)	Required
Tunnel-Private-Group-ID	This attribute indicates group ID for a particular tunneled session.	A string (VID)	Required

A summary of the Tunnel-Private-Group-ID Attribute format is shown below.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a "VLAN Name". Then it will check that it can find out a matched VLAN Name.

NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X authentication is successful, the port will be assigned to VLAN 3. However if the user does not configure the VLAN attributes, when the port is not guest VLAN member, it will be kept in its current authentication VLAN, and when the port is guest VLAN member, it will be assigned to its original VLAN.

Appendix D - IETF RADIUS Attributes Support

Remote Authentication Dial-In User Service (RADIUS) attributes carry specific authentication, authorization, information, and configuration details for the request and reply. This appendix lists the RADIUS attributes currently supported by the Switch.

RADIUS attributes are supported by the IETF standard and Vendor-Specific Attribute (VSA). VSA allows the vendor to create an additionally owned RADIUS attribute. For more information about D-Link VSA, refer to the **RADIUS Attributes Assignment** Appendix.

IETF standard RADIUS attributes are defined in the RFC 2865 Remote Authentication Dial-In User Service (RADIUS), and RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF **RADIUS Authentication Attributes** supported by the D-Link Switch.

Number	IETF Attribute
1	User-Name
2	User-Password
3	CHAP-Password
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
7	Framed-Protocol
8	Framed-IP-Address
12	Framed-MTU
18	Reply-Message
24	State
26	Vendor-Specific
27	Session-Timeout
29	Termination-Action
30	Called-Station-ID
31	Calling-Station-ID
32	NAS-Identifier
60	CHAP-Challenge
61	NAS-Port-Type
64	Tunnel-Type
65	Tunnel-Medium-Type
77	Connect-Info
79	EAP-Message
80	Message-Authenticator
81	Tunnel-Private-Group-ID
85	Acct-Interim-Interval
87	NAS-Port-ID
95	NAS-IPv6-Address