D-Link®
Building Networks for People

CLI Reference Guide

Product Model: DXS-3600 Series
Layer 2/3 Managed 10Gigabit Ethernet Switch
Release 2.00

Table of Contents

1. Introduction

This manual's command descriptions are based on the software release 2.00. The commands listed here are the subset of commands that are supported by the DXS-3600 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 the primary management interface to the DXS-3600 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 the experience 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 either from the CD, bundled with this switch, or from the D-Link website. Other documents related to this switch are:

- *DXS-3600 Series Hardware Installation Guide*
- *DXS-3600 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-3600-32S switch in the DXS-3600 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.

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 commands functionality.
- **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.
- **Command Default Level** – The user privilege level in which the command can be issued.
- **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 both the mode the user is currently in and their privilege level. For each case, 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 five pre-defined privilege levels:

- **Basic User** - Privilege Level 1. This user account level has the lowest priority of the user accounts. The purpose of this type of user account level is for basic system checking.
- **Advanced User** - Privilege Level 3. This user account level is allowed to configure the terminal control setting. This user account can only show limited information that is not related to security.
- **Power User** - Privilege 8. This user account level can execute fewer commands than operator, including configuration commands other than the operator level and administrator level commands.
- **Operator** - Privilege Level 12. This user account level is used to grant system configuration rights for users who need to change or monitor system configuration, except for security related information such as user accounts and SNMP account settings, etc.

- **Administrator** - Privilege Level 15. This administrator user account level can monitor all system information and change any of the system configuration settings expressed in this configuration guide.

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

- **User EXEC Mode**
- **Privileged EXEC Mode**
- **Global Configuration Mode**

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

When a user logs in to the switch, the privilege level of the user determines the command mode the user will enter after initially logging in. The user will either log into **User EXEC Mode** or the **Privileged EXEC Mode**.

- Users with a **basic** user level will log into the switch in the **User EXEC Mode**.
- Users with **advanced** user, power-user, operator or administrator level accounts will log into the switch in the **Privileged EXEC Mode**.

Therefore, the User EXEC Mode can operate at a basic user level and the Privileged EXEC Mode can operate at the advanced user, power-user, operator, or administrator levels. The user can only enter the Global Configuration Mode from the Privileged EXEC Mode. The Global Configuration Mode can be accessed by users who have operator or administrator level user accounts.

As for sub-configuration modes, a subset of those can only be accessed by users who have the highest secure administrator level privileges.

The following table briefly lists the available command modes. Only the basic command modes and some of the sub-configuration modes are enumerated. The basic command modes and basic sub-configuration modes are further described in the following chapters. Descriptions for the rest of the sub-configuration modes are not provided in this section. For more information on the additional sub-configuration modes, the user should refer to the chapters relating to these functions.

The available command modes and privilege levels are described below:

Command Mode/ Privilege Level	**Purpose**
User EXEC Mode / Basic User level	This level has the lowest priority of the user accounts. It is provided only to check basic system settings.
Privileged EXEC Mode / Advanced User level	This level is allowed to configure the terminal control setting. This user account can only show limited information that is not related to security.
Privileged EXEC Mode / Power User level	This level can execute less commands than operator, include the configure commands other than the operator level and administrator level commands.
Privileged EXEC Mode / Operator level	For changing both local and global terminal settings, monitoring, and performing certain system administration tasks. The system administration tasks that can be performed at this level except for any security related information.
Privileged EXEC Mode /	This level is identical to privileged EXEC mode at the operator level,

Administrator level	except that a user at the administrator level can monitor and clear security related settings.
Global Configuration Mode / Operator level	For applying global settings, except for security related settings, on the entire switch. In addition to applying global settings on the entire switch, the user can access other sub-configuration modes from global configuration mode.
Global Configuration Mode / Administrator level	For applying global settings on the entire switch. In addition to applying global settings on the entire switch, the user can access other sub-configuration modes from global configuration mode.
Interface Configuration Mode / Administrator level	For applying interface related settings.
VLAN Interface Configuration Mode	For applying VLAN interface related settings.
VLAN Configuration Mode	For applying settings to a VLAN.
IP Access-List Configuration Mode	For specifying filtering criteria for an IP access list.

User EXEC Mode at Basic User Level

This command mode is mainly designed for checking basic system settings. This command mode can be entered by logging in as a basic user.

Privileged EXEC Mode at Advanced User Level

This command mode is mainly designed for checking basic system settings, allowing users to change the local terminal session settings and carrying out basic network connectivity verification. One limitation of this command mode is that it cannot be used to display information related to security. This command mode can be entered by logging in as an advanced user.

Privileged EXEC Mode at Power User Level

User logged into the switch in privileged EXEC mode at this level can execute fewer commands than operator, including the configuration commands other than the operator level and administrator level commands. The method to enter privileged EXEC mode at power user level is to login to the switch with a user account that has a privileged level of 8.

Privileged EXEC Mode at Operator Level

Users logged into the switch in privileged EXEC mode at this level can change both local and global terminal settings, monitor, and perform system administration tasks (except for security related information). The method to enter privileged EXEC mode at operator level is to login to the switch with a user account that has a privilege level of 12.

Privileged EXEC Mode at Administrator Level

This command mode has a privilege level of 15. Users logged in with this command mode can monitor all system information and change any system configuration settings mentioned in this Configuration Guide. The method to enter privileged EXEC mode at administrator level is to login to the switch with a user account that has a privilege level of 15.

Global Configuration Mode

The primary purpose of the global configuration mode is to apply global settings on the entire switch. Global configuration mode can be accessed at advanced user, power user, operator or administrator level user accounts. However, security related settings are not accessible at advanced user, power user or operator user accounts. In addition to applying global settings on the entire switch, the user can also access other sub-configuration modes. In order to access the global configuration mode, the user must be logged in with the corresponding account level and use the **configure terminal** command in the privileged EXEC mode.

In the following example, the user is logged in as an Administrator in the Privileged EXEC Mode and uses the **configure terminal** command to access the Global Configuration Mode:

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

The **exit** command is used to exit the global configuration mode and return to the privileged 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.

Interface Configuration Mode

Interface configuration mode is used to configure the parameters for an interface or a range of interfaces. An interface can be a physical port, VLAN, or other virtual interface. Thus, interface configuration mode is distinguished further according to the type of interface. The command prompt for each type of interface is slightly different.

VLAN Interface Configuration Mode

VLAN interface configuration mode is one of the available interface modes and is used to configure the parameters of a VLAN interface.

To access VLAN interface configuration mode, use the following command in global configuration mode:

```
Switch(config)# interface vlan 1
Switch(config-if)#
```

Creating a User Account

By default, there is no user account created on this switch. For security reasons, it is highly recommended to create user accounts to manage and control access to this switch's interface. This section will assist a user with creating a user account by means of the Command Line Interface.

Observe the following example.

```
Switch#enable
Switch# configure terminal
Switch(config)# username admin password admin
Switch(config)# username admin privilege 15
Switch(config)# line console
Switch(config-line)#login local
Switch(config-line)#
```

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

- Starting in the User EXEC Mode we enter the command **enable** to access the Privileged EXEC Mode.
- After accessing the Privileged EXEC Mode, we entered the command **configure terminal** to access the Global Configuration Mode. The **username** command can be used in the Global Configuration Mode.
- The command **username admin password admin** creates a user account with the username of *admin* and a password of *admin*.
- The command **username admin privilege 15** assigns a privilege level value of 15 to the user account admin.

- The command **line console** allows us to access the console interface's Line Configuration Mode.
- The command **login local** tell the switch that users need to enter locally configured login credentials to access the console interface.

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 was rebooted, or when the users logs out and back in, the newly created username and password must be entered to access the CLI interface again, as seen below.

```
                    DXS-3600-32S TenGigabit Ethernet Switch

                          Command Line Interface
                         Firmware: Build 2.00.012
          Copyright(C) 2013 D-Link Corporation. All rights reserved.

User Access Verification

Username:admin
Password:*****

Switch#
```

Interface Notation

When configuration the physical ports available on this switch, a specific interface notation is used. The following will explain the layout, terminology and use of this notation.

In the following example, we'll enter the Global Configuration Mode and then enter the Interface Configuration Mode, using the notation **1/0/1**. After entering the Interface Configuration Mode for port 1, we'll change the speed to 1 Gbps, using the **speed 1000** command.

```
Switch# configure terminal
Switch(config)# interface Ethernet 1/0/1
Switch(config-if)# speed 1000
Switch(config-if)#
```

In the above example the notation **1/0/1** was used. The terminology for each parameter is as follows:

- Interface Unit's ID / Open Slot's ID / Port's ID

The Interface Unit's ID is the ID of the stacking unit without the physical stack. If stacking is disabled or this unit is a stand-alone unit, then this parameter is irrelevant. The Open Slot's ID is the ID of the module plugged into the open module slot of the switch. The DXS-3600 Series switch doesn't support any open modules slots, thus this parameters will always by zero for this switch series. Lastly, the Port's ID is the physical port number of the port being configured.

In summary the above example will configure the stacked switch with the ID of 1, with the open slot ID of 0, and the physical port number 1.

Error Messages

When the 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 to 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 # DEVICE
# DEVICE
configure terminal
end

# AAA

configure terminal
# AAA START
no aaa new-model
# AAA END
end

Switch#
```

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

```
Switch#show running-config | include # DEVICE
# DEVICE

Switch#
```

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

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

Current configuration : 56102 bytes
```

```
#------------------------------------------------------------------------------
#                   DXS-3600-32S TenGigabit Ethernet Switch
#                               Configuration
#
#                           Firmware: Build 2.00.012
#           Copyright(C) 2013 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------

# STACK

##  stacking config information
##   #Box                  Prio-
##   #ID    Type      Exist rity
##   #--- ----------- ----- -----
##   #  1 DXS-3600-32S exist 32
##   #  2 DXS-3600-16S no
##   #  3 NOT_EXIST no
##   #  4 NOT_EXIST no
end
end

configure terminal
end

# AAA

configure terminal
# AAA START
no aaa new-model
# AAA END
end

Switch#
```

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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The help 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
   argument.
2. Helpis 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              reconfig            rename

Switch# re
```

The following example shows how to use the **command syntax** help to display the next argument of a partially complete IP access-list standard 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# ip access-list standard ?

<1-1999>             Standard IP access-list number
WORD                 Access-list name

Switch# ip access-list standard
```

2-2 enable

This command is used to enter the Privileged EXEC Mode.

enable [*PRIVILEGE-LEVEL***]**

Parameters

PRIVILEGE-LEVEL	(Optional) Specifies to set the privilege level for the user. The privilege level is between 1 and 15. If **not** specified, level 15 will be used.

Default

None.

Command Mode

User EXEC Mode.

Privilege EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Execute this command if the current level is lower than the command level. If the privileged level requires a password, enter it in the field provided. However, only three attempts are allowed. Failure to access this level returns the user to the current level.

Example

This example shows how to enter the Privileged EXEC Mode.

```
Switch# enable 15
password:***
```

```
Switch#
```

2-3 disable

This command is used to downgrade to a level lower user level than the privileged level.

disable [*PRIVILEGE-LEVEL***]**

Parameters

PRIVILEGE LEVEL	Specifies the privilege level to enter. If not specified, level 1 is used.

Default

None.

Command Mode

User EXEC Mode.

Privilege EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to enter the privilege level, which is lower than the current level. When using this command to enter the privilege level, that has a password configured, no password is needed.

Example

This example shows how to logout.

```
Switch# disable
Switch# logout
```

2-4 configure terminal

This command is used to enter the Global Configuration Mode.

configure terminal

Parameters

None.

Default

None

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enter the Global Configuration Mode.

Example

This example shows how to enter into Global Configuration Mode.

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

2-5 login (EXEC)

This command is used to configure a login username.

login

Parameters

None.

Default

None.

Command Mode

User EXEC Mode.

Privileged EXEC Mode.

Command Default Level

Level: 1.

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 login with username "user1".

```
Switch# login

Username: user1
Password: xxxxx

Switch#
```

2-6 login (Line)

This command is used to set the line login method. Use the **no** form of the command to disable the login.

login [local]

no login

Parameters

login	Specifies that the line login method will be login.
local	Specifies that the line login method will be local.

Default

By default, there is no login details configured for the **console** line.

By default, there is a login method (by password) configured for the **Telnet** line.

By default, there is a login local method (by username and password) configured for the **SSH** line.

Command Mode

Line Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

For Console and Telnet access, when AAA is enabled, the line uses rules configured by the AAA module. When AAA is disabled, the line uses the following authentication rules:

- When login is disabled, the user can enter the line at Level 1.
- When the **by password** option is selected, after inputting the same password as the command password, the user enter the line at level 1. If the password wasn't previously configured an error message will be displayed and the session will be closed.
- When the **username and password** option is selected, enter the username and password configured by the **username** command.

For SSH access, there are three authentication types:

- SSH public key,
- Host-based authentication, and
- Password authentication.

The SSH public key and host-based authentication types are independent from the login command in the line mode. If the authentication type is password, the following rules apply:

- When AAA is enabled, the AAA module is used.
- When AAA is disabled, the following rules are used:
  - When login is disabled, the username and password is ignored. Enter the details at Level 1.
  - When the **username and password** option is selected, use the username and password setup by the username command.
  - When the **password** option is selected, the username is ignored but a password is required using the password command to enter the line at level 1.

Example

This example shows how to enter the Line Configuration Mode and to create a password for the line user. This password only takes effect once the corresponding line is set to login.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# password loginpassword
Switch(config-line)#
```

This example shows how to configure the line console login method as "login".

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

```
Switch(config-line)# login
Switch(config-line)#
```

This example shows how to enter the login command. The device will check the validity of the user from the **password create** command. If correct, the user will have access at the particular level.

```
Switch#login

Password:*************

Switch#
```

This example shows how to create a username “useraccount” with the password of “pass123” and use Privilege 12.

```
Switch# configure terminal
Switch(config)# username useraccount privilege 12 password 0 pass123
Switch(config)#
```

This example shows how to configure the login method as login local.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# login local
Switch(config-line)#
```

2-7 logout

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

logout

Parameters

None.

Default

None.

Command Mode

User EXEC Mode.

Privilege EXEC Mode.

Command Default Level

Level:1.

Usage Guideline

Use this command to close an active terminal session by logging out of the device.

Example

This example shows how to logout

```
Switch# disable
```

```
Switch# logout
```

2-8 end

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

end

Parameters

None.

Default

None.

Command Mode

Any Configurable Mode.

Command Default Level

Level: 1.

Usage Guideline

Executing this command will 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 Privileged EXEC Mode.

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

2-9 exit

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

exit

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 Privilege 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)#
```

2-10 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

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

The function key instructions, below, displays how to navigate the command 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#
```

2-11 password-recovery

This command is used to recover the password related settings. Use the password recovery command in the reset configuration mode.

password-recovery

Parameters

None.

Default

None.

Command Mode

Reset Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Under certain circumstances, the administrator may have the need to update a user's account because the password of the account was forgotten. To do this, the administrator has to enter the **Reset Configuration Mode**. For assistance on how to enter the reset configuration mode, please contact the technical support personnel.

After entering the reset configuration mode, use the **password-recovery** command and follow the confirmation prompt message to recover the password related settings.

Password recovery basically does the following three things:

- Update an existing user account by entering the username of an existing user and its new password or add a new user account with a privileged level of 15. The new user account cannot be created if the maximum number of user accounts is exceeded.
- Update the enabled password for the administrator-privileged level.
- Disable the AAA function to let the system do local authentication.

The updated setting will be saved in the running configuration file. Before the reload is executed, the switch will prompt the administrator to approve saving the running configuration as the startup configuration.

Example

This example shows how to use the password recovery feature.

```
Switch(reset-config)# password-recovery

This command will guide you to do the password recovery procedure.
Do you want to update the user account? (y/n) [n]y
Please input user account: user1
Please input user password:
Do you want to update the enable password for privilege level 15? (y/n) [n]y
Please input privilege level 15 enable password:
```

```
Do you want to disable AAA function to let the system do the local authentication?
(y/n) [n] y

Switch(reset-config)#
```

2-12 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If a specific type is not 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:
Unit     Temperature Descr/ID          Current/Threshold Range
-----   ----------------------------------------------------
1        Central Temperature/1         25C/11~79C
Status code: * temperature is out of threshold range

Detail Fan Status:
------------------------------------------------------------
Unit 1:
  Fan 1 (OK)     Fan 2 (OK)     Fan 3 (OK)

Detail Power Status:
Unit    Power Module      Power Status
-----   ---------------  -------------
1       Internal Power    in-operation
1       External Power    empty
```

```
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.

2-13 show unit

This command is used to display information about system units.

show unit [*UNIT-ID***]**

Parameters

UNIT-ID	(Optional) Specify the unit to display.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays information about the system modules. If no option is specified, then all of units' information will be displayed.

Example

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

```
Switch# show unit

Unit         Model Descr                            Model Name
----  ---------------------------------------  ------------------
 1     24P tenGigabitEthernet                     DXS-3600-32S

Unit         Serial-Number                Status        Up Time
----  --------------------------------  ---------  -----------------
 1     R3I21CA000119                     ok          0DT0H0M51S

Unit   Memory     Total       Used        Free
----  --------  ----------  ----------  ----------
 1     DRAM     2097152 K    744721 K   1352431 K
 1     FLASH    1048064 K     28070 K   1019994 K

Switch#
```

2-14 show cpu utilization

This command is used to display the CPU utilization information.

show cpu utilization

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the system's CPU utilization information 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 -   8 %         One minute -   8 %         Five minutes -   8 %

Switch#
```

2-15 show version

This command is used to display the switch's software version information.

show version

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays version information about the switch.

Example

This example shows how to displays version information about the switch.

```
Switch# show version

System MAC Address: 00-17-9A-14-6B-10

Unit ID    Module Name            Versions
-------  ------------------  ---------------------
   1      DXS-3600-32S        H/W:B1
                              Bootloader:1.10.008
                              Runtime:2.00.012

Switch#
```

2-16 environment temperature threshold

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

environment temperature threshold unit *UNIT-ID* **thermal** *THREMAL-ID* **[high** *VALUE***] [low** *VALUE***]**

no environment temperature threshold unit *UNIT-ID* **thermal** *THREMAL-ID* **[high] [low]**

Parameters

unit *UNIT-ID*	Specifies the unit ID.
thermal *THERMAL-ID*	Specifies the thermal sensor's ID.
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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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 for thermal sensor ID 1 on unit 1.

```
Switch# configure terminal
Switch(config)# environment temperature threshold unit 1 thermal 1 high 100 low 20
Switch(config)#
```

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

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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 the Ethernet port 1/0/1.

```
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 the command to reset 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.

Command Default Level

Level: 12.

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**, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, then 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**, then the port can receive and transmit EAPOL packets only. All user traffic is blocked before authentication. If the control direction is set to **in**, then in addition to receiving and transmitting EAPOL packets, the port can transmit user traffic but not receive user traffic before authentication.

Example

This example shows how to configure the controlled direction of the traffic through Ethernet eth1/0/1 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

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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 1/0/1.

```
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** 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.

Command Default Level

Level: 12.

Usage Guideline

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

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**, then the access to the port for the controlled direction needs to be authenticated. If the port control is set to **force-unauthorized**, then the access to the port for the controlled direction is blocked.

Example

This example shows how to deny all access on Ethernet port 1/0/1.

```
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 the 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.

Command Default Level

Level: 12.

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 separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
mac-address *MAC-ADDRESS*	Specifies the MAC address to be initialized.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Under 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 Ethernet port 1/0/1.

```
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 the command to reset 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.

Command Default Level

Level: 12.

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 Ethernet port 1/0/1 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.

Command Default Level

Level: 12.

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 Ethernet port 1/0/1 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 Ethernet port 1/0/1.

```
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 separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
mac-address *MAC-ADDRESS*	Specifies the MAC address to re-authenticate.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Example

This example shows how to re-authenticate Ethernet port 1/0/1.

```
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 a switch. Use the **no** form of this command to return to disable IEEE 802.1X authentication function.

dot1x system-auth-control

no dot1x system-auth-control

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 a 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 the command to revert a specific timer setting to the default value.

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, authenticator will send EAP-Request packet to 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 the supplicant messages other than 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.

Command Default Level

Level: 12.

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 Ethernet port 1/0/1 to be 15, 15, and 10 seconds, respectively.

```
Switch# 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. If not specified, the global configuration will be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display the global configuration or interface configuration. If the configuration command is entered without parameters, the global configuration will be displayed. Otherwise, the configuration on the specified interface will be displayed.

Example

This example shows how to display the dot1X global configuration.

```
Switch# show dot1x

802.1X                      : Enabled

Switch#
```

This example shows how to display the dot1X configuration on Ethernet port 1/0/1.

```
Switch# 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. If no interface is specified, information about all interfaces will be displayed.

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. If not specified, information about all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display 802.1X diagnostics. Using this command without parameters will display information about all interfaces. Otherwise, the diagnostics on the specified interface will be displayed.

Example

This example shows how to display the dot1X diagnostics on Ethernet port 1/0/1.

```
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. If no interface is specified, information about all interfaces will be displayed.

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. If not specified, information about all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display 802.1X statistics. Using this command without parameters will display information about all interfaces. Otherwise, the statistics on the specified interface will be displayed.

Example

This example shows how to display dot1X statistics on Ethernet port 1/0/1.

```
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 display IEEE 802.1X session statistics. If no interface specified, information about all interfaces will be displayed.

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. If not specified, information about all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display 802.1X session statistics. Using this command without parameters will display information about all interfaces. Otherwise, the session statistics on the specified interface will be displayed.

Example

This example shows how to display dot1X session statistics on Ethernet port 1/0/1.

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

eth6/0/1 session statistic counters are following:
SessionOctetsRX                         : 0
SessionOctetsTX                         : 0
SessionFramesRX                         : 0
SessionFramesTX                         : 0
SessionId                               :
SessionAuthenticationMethod             : Remote Authentication Server
SessionTime                             : 0
SessionTerminateCause                   :SupplicantLogoff
SessionUserName                         :

Switch#
```

4. Access Control List (ACL) Commands

4-1 access-list resequence

This command is used to re-sequence the sequence number of the access list entries in an access list. Use the **no** form of the command to reset 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.

Command Default Level

Level: 12.

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, then 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 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# configure terminal
Switch(config)# show access-list ip R&D
Extended IP access list R&D(ID: 3552)
10 permit tcp any 10.20.0.0 255.255.0.0
```

```
20 permit tcp any host 10.100.1.2
30 permit icmp any any
Switch(config)# ip extended access-list R&D
Switch(config-ip-ext-acl)# 5 permit tcp any 10.30.0.0 255.255.0.0
Switch(config-ip-ext-acl)# exit
Switch(config)# show access-list ip R&D
Extended IP access list R&D(ID: 3552)5 permit tcp any 10.30.0.0 255.255.0.0
10 permit tcp any 10.20.0.0 255.255.0.0
20 permit tcp any host 10.100.1.2
30 permit icmp any any
Switch(config)# access-list resequence R&D 1 2
Switch(config)# show access-list ip R&D
Extended IP access list R&D(ID: 3552)
1 permit tcp any 10.30.0.0 255.255.0.0
3 permit tcp any 10.20.0.0 255.255.0.0
5 permit tcp any host 10.100.1.2
7 permit icmp any any
Switch(config)#
```

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 or access map for the VLAN filter function. Use the **no** form of the command to disable the ACL hardware counter function.

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

no acl-hardware-counter {access-group {*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***} | vlan-filter** *ACCESS-MAP-NAME***}**

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.
vlan-filter *ACCESS-MAP-NAME*	Specifies the name of the access map to be configured.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command with parameter **access-group** will 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.

The command with parameter **vlan-filter** will enable the ACL hardware counter for all VLAN(s) that have applied the specified VLAN access-map. The number of packets that permitted by each access map are counted.

Example

This example shows how to enable the ACL hardware counter.

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

4-3 action

This command is used to configure the forward, drop, or redirect action of the sub-map in the VLAN access-map sub-map configuration mode. Use the **no** command to reset to the default action.

action {forward | drop | redirect *INTERFACE-ID***}**

no action

Parameters

forward	Specifies to forward the packet when matched.
drop	Specifies to drop the packet when matched.
redirect *INTERFACE-ID*	Specifies the interface ID for the redirection action. Only physical ports are allowed to be specified.

Default

By default, the action is **forward**.

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

One sub-map has only one action. The action configured later overwrites the previous action. A VLAN access map can contain multiple sub-maps. The packet that matches a sub-map (a packet permitted by the associated access-list) will take the action specified for the sub-map. No further checking against the next sub-maps is done. If the packet does not match a sub-map, then the next sub-map will be checked.

Example

This example shows how to configure the action in the sub-map.

```
Switch# show vlan access-map
VLAN access-map vlan-map 20
  match mac address: ext_mac(ID: 6856)
  action: forward
Switch# configure terminal
```

```
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)# action redirect eth1/0/5
Switch(config-access-map)# end
Switch# show vlan access-map
VLAN access-map vlan-map 20
  match mac address:  ext_mac(ID: 6856)
  action: redirect eth1/0/5
Switch#
```

4-4 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***] | vlan-filter [***ACCESS-MAP-NAME***]}**

Parameters

access-group *ACCESS-LIST-NAME*	Specifies the name of the access list to be cleared.
access-group *ACCESS-LIST-NUMBER*	Specifies the number of the access list to be configured.
vlan-filter *ACCESS-MAP-NAME*	Specifies the name of the access map to be cleared.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If no access-list name or number is specified with the parameter **access-group**, all access-group hardware counters will be cleared. If no access-map name is specified with the parameter **vlan-filter**, all VLAN filter hardware counters will be cleared.

Example

This example shows how to clear the ACL hardware counter.

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

4-5 expert access-group

This command is used to apply a specific expert ACL to an interface. Use the **no** command to cancel the application.

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

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

Parameters

NAME	Specifies the name of the expert access-list to be configured. The name can be up to 32 characters.
NUMBER	Specifies the number of the expert access list to be configured.
in	(Optional) Specifies to filter the incoming packets of the interface. If the direction is not specified, **in** is used.
out	(Optional) Specifies to filter the outgoing packets to transmit to the interface.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If expert 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.

Example

This example shows how to apply an expert ACL to an interface. The purpose is to apply the ACL **exp_acl** on the Ethernet port 1/0/2 to filter the incoming packets.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# expert access-group exp_acl in
Switch(config-if)# end
Switch# show access-group interface eth1/0/2
eth1/0/2:
  Inbound expert access-list : exp_acl(ID: 8999)
Switch#
```

4-6 expert access-list

This command is used to create or modify an extended expert ACL. This command will enter into the extended expert access-list configuration mode. Use the **no** command to remove an extended expert access-list.

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

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

Parameters

NAME	Specifies the name of the extended expert access-list to be configured. The name can be up to 32 characters.
NUMBER	(Optional) Specifies the ID number of expert access list. For extended expert access lists, the value is from 8000 to 9999.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 expert access list numbers will be assigned automatically.

Example

This example shows how to create an extended expert ACL.

```
Switch# configure terminal
Switch(config)# expert access-list extended exp_acl
Switch(config-exp-nacl)# end
Switch# show access-list
Access-List-Name                        Type
--------------------------------------- ---------------
exp_acl(ID: 8999)                       expert ext-acl

Total Entries: 1

Switch#
```

4-7 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 maximum length is 32 characters.
NUMBER	Specifies the number of the IP access list to be applied.
in	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	Specifies that the IP access list will be applied to check packets in the

	egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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, then 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, then 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 an Ethernet port 6/0/2.

```
Switch# configure terminal
Switch(config)# interface eth6/0/2
Switch(config-if-gi)#ip access-group Strict-Control
The remaining applicable IP related access entries are 2500
The remaining applicable port operators are 10
Switch(config-if-gi)#
```

4-8 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** 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 without this option the IP access list is a standard IP access list. When using the extended option, more fields can be chosen for the filter.
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	(Optional) 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.

Command Default Level

Level: 12.

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 10.20.0.0 255.255.0.0
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)#
```

4-9 ipv6 access-group

This command is used to specify the IPv6 access list to be applied to an interface. Use the **no** 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.
NUMBER	Specifies the number of the IPv6 access list to be applied.
in	Specifies that the IPv6 access list will be applied to check in the ingress direction. If the direction is not specified, **in** is used.
out	Specifies that the IPv6 access list will be applied to check in the egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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, then 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, then an error message will be displayed.

Example

This example shows how to specify the IPv6 access list “ip6-control” as an IP access group for eth3/0/3.

```
Switch# configure terminal
Switch(config)# interface eth3/0/3
Switch(config-if)# ipv6 access-group ip6-control in
The remaining applicable IPv6 related access entries are 2500
The remaining applicable port operators are 10
Switch(config-if)#
```

4-10 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

NAME	Specifies the name of the IPv6 access list to be configured. The maximum length is 32 characters.
NUMBER	(Optional) 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.
extended	(Optional) Specifies that without this option the IPv6 access list is a standard IPv6 access list. When using the extended option, the IPv6 access list is an extended IPv6 access list and more fields can be chosen for the filter.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 IPv6 extended 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)#
```

4-11 list-remark

This command is used to add remarks for the specified ACL. Use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

This command is available in the MAC, IP, IPv6, and Expert Access-list Configure mode.

Example

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

```
Switch# configure terminal
Switch(config)# ip extended access-list 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#
```

4-12 mac access-group

This command is used to specify a MAC access list to be applied to an interface. Use the **no** 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 in the egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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, then an error message will be displayed.

Example

This example shows how to apply the MAC access list daily-profile to Ethernet port 5/0/1.

```
Switch# configure terminal
Switch(config)# interface eth5/0/1
Switch(config-if-gi)# mac access-group daily-profile in
The remaining applicable MAC access entries are 204
Switch(config-if-gi)#
```

4-13 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** command to delete a MAC access list.

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

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

Parameters

NAME	Specifies the name of the MAC access-list to be configured. The maximum length is 32 characters.
NUMBER	(Optional) 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.

Command Default Level

Level: 12.

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)#
```

4-14 match ip address

This command is used to associate an IP access list for the configured sub-map. The **no** form of this command removes the match entry.

match ip address {*ACL-NAME* **|** *ACL-NUMBER***}**

no match ip address

Parameters

ACL-NAME	Specifies the name of the ACL access list to be configured. The name can be up to 32 characters.
ACL-NUMBER	Specifies the number of the IP ACL access list to be configured.

Default

None.

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to associate an IP access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list or MAC access list). IP sub-map just checks IP packets. The newer command overwrites the previous setting.

Example

This example shows how to configure the match content in the sub-map.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)# match ip address sp1
Switch(config-access-map)# end
Switch# show vlan access-map

VLAN access-map vlan-map 20
  match ip address:  sp1(ID: 1999)
  action: forward

Switch#
```

4-15 match ipv6 address

This command is used to associate IPv6 access lists for the configured sub-maps. The **no** form of this command removes the match entry.

match ipv6 address {*ACL-NAME* **|** *ACL-NUMBER***}**

no match ipv6 address

Parameters

ACL-NAME	Specifies the name of the IPv6 ACL access list to be configured. The name can be up to 32 characters.
ACL-NUMBER	Specifies the number of the IPv6 ACL access list to be configured.

Default

None.

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to associate an IPv6 access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list or MAC access list). IPv6 sub-map just checks IPv6 packets. The later command overwrites the previous setting.

Example

This example shows how to set the match content in the sub-map.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)# match ipv6 address sp1
Switch(config-access-map)# end
Switch# show vlan access-map

VLAN access-map vlan-map 20
  match ipv6 address:  sp1(ID: 12999)
  action: forward

Switch#
```

4-16 match mac address

This command is used to associate MAC access lists for the configured sub-maps. The **no** form of this command removes the match entry.

match mac address {*ACL-NAME* **|** *ACL-NUMBER***}**

no match mac address

Parameters

ACL-NAME	Specifies the name of the ACL MAC access list to be configured. The name can be up to 32 characters.
ACL-NUMBER	Specifies the number of the ACL MAC access list to be configured.

Default

None.

Command Mode

VLAN Access-map Sub-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to associate a MAC access list with the configured sub-map. One sub-map can only be associated with one access list (IP access list, IPv6 access list or MAC access list). MAC sub-map just check non-IP packets. The later command overwrites the previous setting.

Example

This example shows how to set the match content in the sub-map.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 30
Switch(config-access-map)# match mac address ext_mac
```

```
Switch(config-access-map)# end
Switch# show vlan access-map

VLAN access-map vlan-map 20
  match ip address:  sp1(ID: 3999)
  action: forward
VLAN access-map vlan-map 30
  match mac address:  ext_mac(ID: 7999)
  action: forward

Switch#
```

4-17 permit | deny (expert access-list)

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

Extended Expert ACL:

[*SEQUENCE-NUMBER***] {permit | deny}** *PROTOCOL* **{***SRC-IP-ADDR SRC-IP-WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC-ADDR* **| any} {***DST-IP-ADDR DST-IP-WILDCARD* **| host** *DST-IP-ADDR* **| any} {***DST-MAC-ADDR DST-MAC-WILDCARD* **| host** *DST-MAC-ADDR* **| any} [cos** *OUTER-COS* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-VLAN***]] [fragments] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} tcp {***SRC-IP-ADDR SRC-IP-WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC-ADDR* **| any} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] {***DST-IP-ADDR DST-IP-WILDCARD* **| host** *DST-IP-ADDR* **| any} {***DST-MAC-ADDR DST-MAC-WILDCARD* **| host** *DST-MAC-ADDR* **| any} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] [***TCP-FLAG***] [cos** *OUTER-COS* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-VLAN***]] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} udp {***SRC-IP-ADDR SRC-IP-WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC-ADDR* **| any} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] {***DST-IP-ADDR DST-IP-WILDCARD* **| host** *DST-IP-ADDR* **| any} {***DST-MAC-ADDR DST-MAC-WILDCARD* **| host** *DST-MAC-ADDR* **| any} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] [cos** *OUTER-COS* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-VLAN***]] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} icmp {***SRC-IP-ADDR SRC-IP-WILDCARD* **| host** *SRC-IP-ADDR* **| any} {***SRC-MAC-ADDR SRC-MAC-WILDCARD* **| host** *SRC-MAC-ADDR* **| any} {***DST-IP-ADDR DST-IP-WILDCARD* **| host** *DST-IP-ADDR* **| any} {***DST-MAC-ADDR DST-MAC-WILDCARD* **| host** *DST-MAC-ADDR* **| any} [***ICMP-TYPE* **[***ICMP-CODE***] | ***ICMP-MESSAGE***] [cos** *OUTER-COS* **[inner** *INNER-COS***]] [vlan** *OUTER-VLAN* **[inner** *INNER-VLAN***]] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [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.
cos *OUTER-COS*	(Optional) Specifies the outer priority value. This value must be between 0 and 7.

inner *INNER-COS*	(Optional) Specifies the inner priority value. This value must be between 0 and 7.
vlan *OUTER-VLAN*	(Optional) Specifies the outer VLAN ID.
inner *INNER-VLAN*	(Optional) Specifies the inner VLAN ID.
any	Specifies to use any source MAC address, any destination MAC address, any source IP address, or any destination IP 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 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.
PROTOCOL	(Optional) Specifies the IP protocol ID.
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.
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.
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.
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.
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) Specifiese 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.
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 following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, echo-request, header, hop-limit, mld-query, mld-reduction, mld-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.

Default

None.

Command Mode

Extended Expert Access-list Configuration Mode.

Command Default Level

Level: 12.

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.

Even if the **fragment** parameter of the **tcp**, **udp** and **icmp** parameters of the **permit | deny (expert access-list)** command is removed, the user can still use the *PROTOCOL* option of the **permit | deny (expert access-list)** command to configure the **fragment** parameter.

Example

This example shows how to use the extended expert ACL. The purpose is to deny all the TCP packets with the source IP address 192.168.4.12 and the source MAC address 00:13:00:49:82:72.

```
Switch# configure terminal
Switch(config)# expert access-list extended exp_acl
Switch(config-exp-nacl)# deny tcp host 192.168.4.12 host 0013.0049.8272 any any
Switch(config-exp-nacl)# end
Switch# show access-lists

Extended Expert access list exp_acl(ID: 9999)
  10 deny tcp host 192.168.4.12 host 0013.0049.8272 any any

Switch#
```

4-18 permit | deny (ip access-list)

This command is used to add a permit or a deny entry. Use the **no** form of the 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***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] [***TCP-FLAG***] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [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***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] [[precedence** *PRECEDENCE***] [tos** *TOS***] | dscp** *DSCP***] [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***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny} {gre | esp | eigrp | igmp | ipinip | ospf | pcp | pim | vrrp | protocol-id** *PROTOCOL-ID***} {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***] [tos** *TOS***] | dscp** *DSCP***] [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***] [tos** *TOS***] | dscp** *DSCP***] [time-range** *PROFILE-NAME***]**

Standard IP Access List:

[*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***]**

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.
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.
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.
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.
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) Specifiese 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.
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.

Command Default Level

Level: 12.

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.

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 extended access-list 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-ip”. 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)#
```

4-19 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***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT***] [***TCP-FLAG***] [dscp** *VALUE***] [flow-label** *FLOW-LABEL***] [time-range** *PROFILE-NAME***]**

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

[*SEQUENCE-NUMBER***] {permit | deny} {esp | pcp | sctp | protocol-id** *PROTOCOL-ID***} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [fragments] [dscp** *VALUE***] [flow-label** *FLOW-LABEL***] [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***] [flow-label** *FLOW-LABEL***] [time-range** *PROFILE-NAME***]**

Standard IPv6 Access List:

[*SEQUENCE-NUMBER***] {permit | deny} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} [any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***]**

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-ADDRIPREFIX-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.
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.
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255.
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.
fragments	(Optional) Specifiese 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.

Command Default Level

Level: 12.

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.

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)#
```

4-20 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 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* **[inner** *INNER-COS***]] [vlan** *VLAN-ID* **[inner** *INNER-VLAN***]] [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 hexidecimal 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.
inner *INNER-COS*	(Optional) Specifies the inner priority value. The range is from 0 to 7.
vlan *VLAN-ID*	(Optional) Specifies the VLAN-ID.
inner *INNER-VLAN*	(Optional) Specifies the inner VLAN ID.
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.

Command Default Level

Level: 12.

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.

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)#
```

4-21 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If interface is not specified, all of the interfaces that have access list configured will be displayed.

Example

This example shows how to display access lists that are applied to all of the interfaces.

```
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#
```

4-22 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***] | expert [***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.
expert	(Optional) Specifies to display a listing of all expert access lists.
NAME | *NUMBER*	Specifies to display the contents of the specified access list.
arp	Specifies to display the ARP access list.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays access list information. If no option 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
```

```
------------------------------------ ---------------
simple-ip-acl(ID: 3998)              ip ext-acl
simple-rd-acl(ID: 3999)              ip ext-acl
rd-mac-acl(ID: 6998)                 mac ext-acl
rd-ip-acl(ID: 1998)                  ip acl
ip6-acl(ID: 12999)                   ipv6 ext-acl
park-arp-acl                         arp acl

Total Entries: 6

Switch#
```

This example shows how to display the IP access list called R&D.

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

IP access list R&D(ID:3996)
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#
```

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

IP access list simple-ip-acl(ID:3994)
10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 12410 packets  Egr: 85201 packets)
20 permit tcp any host 10.100.1.2   (Ing: 6532 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-eth1/0/8
 Egress port(s): eth1/0/3

Switch#
```

4-23 show vlan access-map

This command is used to display the VLAN access-map configuration information.

show vlan access-map [*MAP-NAME***]**

Parameters

MAP-NAME	(Optional) Specifies the name of the VLAN access map being configured. The name can be up to 32 characters.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If no access-map name is specified, all VLAN access-map information will be displayed. If the user enables the ACL hardware counter for an access-map, the counter will be displayed based on each sub-map.

Example

This example shows how to display the VLAN access-map.

```
Switch# show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
action: forward
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 6995)
  action: redirect  eth1/0/5

Switch#
```

This example shows how to display the contents of the VLAN access-map if its hardware counter is enabled.

```
Switch# show vlan access-map

VLAN access-map vlan-map 10
  match ip access list: stp_ip1(ID: 1888)
action: forward
Counter enable on VLAN(s): 1-2
match count: 8541 packets
VLAN access-map vlan-map 20
  match mac access list:  ext_mac(ID: 6995)
action: redirect  eth1/0/5
Counter enable on VLAN(s): 1-2
match count: 5647 packets

Switch#
```

4-24 show vlan filter

This command is used to display the VLAN filter configuration of VLAN interfaces.

show vlan filter [access-map *MAP-NAME* **| vlan** *VLAN-ID***]**

Parameters

MAP-NAME	(Optional) Specifies the name of the VLAN access map. The name can be up to 32 characters.
VLAN-ID	(Optional) Specifies the VLAN ID.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The **show vlan filter access-map** command is used to display the VLAN filter information by access map. The command **show vlan filter vlan** is used to display the VLAN filter information by VLAN.

Example

This example shows how to display VLAN filter information.

```
Switch# show vlan filter

VLAN Map aa
  Configured on VLANs: 5-127,221-333
VLAN Map bb
  Configured on VLANs: 1111-1222

Switch#

Switch# show vlan filter vlan 5

VLAN ID 5
  VLAN Access Map: aa

Switch#
```

4-25 vlan access-map

This command is used to create a sub-map of a VLAN access map and enter the VLAN access-map sub-map configure mode. The **no** form of this command used to delete an access-map or its sub-map.

vlan access-map *MAP-NAME* **[***SEQUENCE-NUM***]**

no vlan access-map *MAP-NAME* **[***SEQUENCE-NUM***]**

Parameters

MAP-NAME	Specifies the name of the VLAN access map to be configured. The name can be up to 32 characters.
SEQUENCE-NUM	(Optional) Specifies the sequence number of the sub-map. The valid range is from 1 to 65535.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A VLAN access map can contain multiple sub-maps. For each sub-map, one access list (IP access list, IPv6 access list or MAC access list) can be specified and one action can be specified. After a VLAN access map is created, the user can use the **vlan filter** command to apply the access map to VLAN(s).

A sequence number will be assigned automatically if the user does not assign it manually, and the automatically assigned sequence number starts from 10, and increase 10 per new entry.

The packet that matches the sub-map (that is packet permitted by the associated access-list) will take the action specified for the sub-map. No further check against the next sub-maps is done. If the packet does not match a sub-map, then the next sub-map will be checked.

Using the **no** form of this command without specify sequence numbers, will delete all sub-map information of the specified access-map.

Example

This example shows how to create a VLAN access map.

```
Switch# configure terminal
Switch(config)# vlan access-map vlan-map 20
Switch(config-access-map)#
```

4-26 vlan filter

This command is used to apply a VLAN access map in a VLAN. Use the **no** command to remove a VLAN access map from the VLAN.

vlan filter *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

no vlan filter *MAP-NAME* **vlan-list** *VLAN-ID-LIST*

Parameters

MAP-NAME	Specifies the name of the VLAN access map.
VLAN-ID-LIST	Specifies the VLAN ID list.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A VLAN can only be associated with one VLAN access map.

Example

This example shows how to apply the VLAN access-map “vlan-map” in VLAN 5.

```
Switch# configure terminal
Switch(config)# vlan filter vlan-map vlan-list 5
Switch(config-access-map)# end
Switch# show vlan filter

VLAN Map vlan-map
  Configured on VLANs: 5

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 the 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.

Command Default Level

Level: 15.

Usage Guideline

This command specifies 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 a standard IP access list is created and is specified 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 banner login

This command is used to enter banner login mode to configure the banner login message. Use the **no** command to revert to the factory default the login banner.

banner login *cMESSAGEc*

no banner login

Parameters

c	Specifies the separator of the login banner message, for example a pound sign (#). The delimiting character is not allowed in the login banner message.
MESSAGE	Specifies the contents of a login banner which will be displayed before the username and password login prompts.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to define a customized banner to be displayed after the user successfully logs into the system. Follow the banner login command with one or more blank spaces and a delimiting character of your choice. Then enter one or more lines of text, terminating the message with the second occurrence of the delimiting character. For example with a pound sign (#) being the delimiting character, after inputting the delimiting character, press the enter key, then the login banner contents can be typed. The delimiting character need to be input then press enter to complete the type. To configure the login banner contents to default, use **no** banner login command in global configuration mode.

Note: The typed additional characters after the end delimiting character are invalid. These characters will be discarded by the system. The delimiting character cannot be used in the login banner text.

Example

This example shows how to configure a login banner. The hash sign (#) is used as the delimiting character. The start delimiting character, banner contents and end delimiting character will be input before press first enter key:

```
Switch# configure terminal
Switch(config)# banner login #Enter Command Line Interface#
Switch(config)#
```

This example shows how to configure a login banner. The hash sign (#) is used as the delimiting character. Just the start delimiting character will be input before press first enter key.

```
Switch# configure terminal
Switch(config)# banner login #
LINE  c banner-text c, where 'c' is a delimiting character
Enter Command Line Interface
#
Switch(config)#
```

5-3 prompt

This command is used to customize the CLI prompt. Use the **no** form of the command to reset the prompt to default setting.

prompt *STRING*

no prompt

Parameters

STRING	Specifies a string to define the customized prompt. The prompt will be based on the specified characters or the following control characters. The space character in the string is ignored. % h – encode the SNMP server name. %s – space %% - encode the % symbol

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the prompt command to customize the CLI prompt. If the user selects to encode the SNMP server name as the prompt, only the first 15 characters are encoded. The privileged level character will appear as the last character of the prompt.

The character is defined as follows.

- '>' Represents user level.
- '#' Represents privileged user level.

Example

This example shows how to change the prompt to "BRANCH A" using administrator.

```
Switch# configure terminal
Switch(config)# prompt BRANCH%sA
BRANCH A(config)#
```

5-4 enable password

This command is used to setup enable password to enter different privileged levels and use the **no** to return the password to the empty string.

enable password [level *PRIVILEGE-LEVEL***] [0| 7]** *PASSWORD*

no enable password [level *PRIVILEGE-LEVEL***]**

Parameters

level *PRIVILEGE-LEVEL*	Specifies the privilege level for the user. The privilege level is between 1 and 15. If this argument is not specified in the command or the no form of the command, the privilege level defaults to 15 (traditional enable privileges).
0 *PASSWORD*	Specifies the password the user must enter to gain access to the

	switch. The password can contain embedded spaces. The password is case-sensitive. This is the default option. The plain-text password maximum length is 32. (The range is 1-32)
7 *PASSWORD*	Specifies the password in the encrypted form based on SHA-I. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive. The syntax is Encrypted Password.

Default

By default, no password is set. It is an empty string.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

The exact password for a specific level needs to be used to enter the privilege level. Each level has only one password to enter the level.

Example

This example shows how to create an **enable** password at the privilege level 15 of “MyEnablePassword”.

```
Switch# configure terminal
Switch(config) #enable password MyEnablePassword
Switch# disable
Switch# enable
Password:****************
Switch# show privilege
Current privilege level is 15
Switch#
```

5-5 ip http server

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

ip http server

no ip http server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables 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)#
```

5-6 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** command to disable the HTTPS server function.

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

no ip http secure-server

Parameters

POLICY-NAME	(Optional) Specifies the SSL service policy name. Use this **ssl-service-policy** keyword only if you have already declared an SSL service policy using the **ssl-service-policy** command. When no keyword is specified, a built-in local certificate will be used for HTTPS.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables the HTTPS server function and uses the specified SSL service policy 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)#
```

5-7 ip http access-class

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

ip http access-class *IP-ACL*

no ip http 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.

Command Default Level

Level: 12.

Usage Guideline

This command specifies an access list to restrict the access to the HTTP server. If the specified access list does not exist, the command does not take effect, thus no access list is checked for the user's access to HTTP.

Example

This example shows how a standard IP access list is created and is specified as the access list to access the HTTP server. Only the host 2265.1.1.1 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)#
```

5-8 ip http service-port

This command is used to specify the HTTP service port. Use the **no** command to return the service port to 80.

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.

Command Default Level

Level: 12.

Usage Guideline

This command configures 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)#
```

5-9 ip telnet server

This command is used to enable a Telnet server. And use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

This command enables or disables 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)#
```

5-10 ip telnet service port

This command is used to specify the service port for Telnet. Use the **no** command to return the service port to 23.

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 value is 23.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command configures 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)#
```

5-11 ip telnet source-interface

This command is used to specify the interface whose IP address will be used as the source address of Telnet packets that initiates a Telnet connection. To remove the specification, use the **no** form of this command.

ip telnet source-interface *INTERFACE-ID*

no ip telnet source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source address of packets that initiates a Telnet connection.

Default

The IP address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the interface IP address source address packets that initiates a Telnet connection.

Example

This example shows how to configure VLAN 100 as the source interface for Telnet packets to initiate a Telnet connection.

```
Switch# configure terminal
Switch(config)# ip telnet source-interface vlan100
Switch(config)#
```

5-12 line

This command is used to identify a line type for configuration and enter 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.

Command Default Level

Level: 12.

Usage Guideline

The line command is used 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)#
```

5-13 service password recovery

This command is used to enable or disable the backdoor password recovery feature. Use the **no** form of the command to disable the backdoor password recovery feature.

service password-recovery

no service password-recovery

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the backdoor password recovery feature which is open by default.

Example

This example shows how to disable the password recovery backdoor feature.

```
Switch# configure terminal
Switch(config)# no service password-recovery
Switch(config)#
```

5-14 service password encryption

This command is used to enable the encryption of the password before stored in the configuration file. The **no** command will disable the encryption.

service password-encryption

no service password-encryption

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level:15.

Usage Guideline

The user account configuration information is stored in the running configuration file and can be applied to the system later. If the **service password-encryption** command is enabled, the password will be stored in the encrypted form.

When the service password encryption option is disabled and the password is specified in the plain text form, the password will be in plain text form. However, if the password is specified in the encrypted form or if the password has been converted to the encrypted form by the last **enable password encryption** command, the password will still be in the encrypted form. It cannot be reverted back to plain text.

The password affected by this command includes the user account password, enable password, and the authentication password.

Example

This example shows how to enable the encryption of the password before stored in the configuration file.

```
Switch# configure terminal
Switch(config)# service password encryption
Switch(config)#
```

5-15 show terminal

This command is used to obtain information about the terminal configuration parameter settings for the current terminal line. Use this command in any EXEC mode or any configuration mode.

show terminal

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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: 9600 bps

Switch#
```

5-16 show users

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

show users

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays information about the active lines on the switch.

Example

This example shows how to display all session information.

```
Switch# show users

Type      User-Name           Privilege Login-Time          IP address
------------------------------------------------------------------------------
* console Anonymous           15        2M57S

Total Entries: 1

Switch#
```

5-17 telnet

This command is used to login another device that supports Telnet.

telnet [/vrf *VRF-NAME***] [***IP-ADDRESS* **|** *IPV6-ADDRESS***] [***TCP-PORT***]**

Parameters

VRF-NAME	Specifies the name of the routing forwarding instance.
IP-ADDRESS	Specifies the IPv4 address of the host.
IPV6-ADDRESS	Specifies the IPv6 address of the host.
TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 0 and 65535. The “well-known” TCP port for the Telnet protocol is 23

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This is the Telnet client function and can be used to communicate with another device using the Telnet feature. The Telnet software supports special Telnet commands in the form of Telnet sequences that map generic terminal control functions to operating system-specific functions. To issue a special Telnet command, enter the escape sequence and then a command character. The default escape sequence is CTRL+_ (press and hold the CTRL and Shift keys and the underscore '_' key). The special Telnet commands will be displayed as follows:

- e – Exits the Telnet connection. Either an uppercase or lowercase letter 'e' can exit the Telnet connection.

If another key is pressed, the terminal will return to the original active Telnet session.

Multiple Telnet sessions can be opened on the switch system and each open Telnet session can have its own Telnet client software supported at the same time

Example

This example shows how to Telnet to the IP address 10.90.90.91 using the default port 23. The IP address, 10.90.90.91 is the DXS-3600-32S management interface which allows a user to login.

```
Switch# telnet 10.90.90.91

                    DXS-3600-32S Gigabit Ethernet Switch

                           Command Line Interface
                          Firmware: Build 2.00.012
          Copyright(C) 2013 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

This example shows how to Telnet through port 23 to 10.90.90.91 and the connection failed. Try using port 3500 instead to login into the management interface.

```
Switch#telnet 10.90.90.91

ERROR: Could not open a connection to host on server port 23.

Switch# telnet 10.90.90.91 3500

                    DXS-3600-32S Gigabit Ethernet Switch

                           Command Line Interface
                          Firmware: Build 2.00.012
          Copyright(C) 2013 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

5-18 terminal length

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

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

Use the EXEC Mode or Privilege EXEC Mode for the **terminal length** command.

Use the Global Configuration Mode for the **terminal length default** command.

Command Default Level

Level: 1 (for the **terminal length** command).

Level: 12 (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, then 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. Valid entries are from 0 to 512. The default is 24 lines. A selection of 0's instructs the Switch to scroll continuously (no pausing).

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#
```

5-19 terminal speed

This command is used to setup the terminal speed. Use the **no** form of the command to reset 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.

Command Default Level

Level: 12.

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)#
```

5-20 session timeout

This command is used to configure the line session timeout value. Use the **no** form of the command to reset it to the default settings.

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.

Command Default Level

Level: 12.

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)#
```

5-21 terminal width

The 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 doesn't affect any current sessions.

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

Use the EXEC Mode or Privilege EXEC Mode for the **terminal width** command.

Use the Global Configuration Mode for the **terminal width default** command.

Command Default Level

Level: 1 (for the **terminal width** command).

Level: 12 (for the **terminal width default** command).

Usage Guideline

By default, the switch's system terminal provides a screen display width of 80 characters. The **terminal width** command changes 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, which is 80 characters.

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 settings take effect.

Example

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

```
Switch# show terminal

Length: 24 lines
```

```
Width: 80 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600

Switch# terminal width 120
Switch# show terminal

Length: 24 lines
Width: 120 columns
Default Length: 24 lines
Default Width: 80 columns
Baud rate: 9600

Switch #
```

5-22 username

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

username *NAME* **[privilege** *LEVEL***] [nopassword | password [0 | 7]** *PASSWORD***]**

no username [*NAME***]**

Parameters

NAME	Specifies the user name with a maximum of 32 characters.
privilege *LEVEL*	Specifies the privilege level for each user. The privilege level must be between 1 and 15.
nopassword	Specifies that there will be no password associated with this account.
password	Specifies the password for the user.
0	Specifies the password in clear, plain text. The password length is between 1 and 32 characters and can contain embedded spaces. It is case-sensitive. If the password syntax cannot be specified, the syntax remains plain text.
7	Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text.
PASSWORD	Specifies the password string based on the type.

Default

By default, no username-based authentication system is established.

If not specified, use 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command creates user accounts with different access levels. When the user login with Level 1, the user will be in the User EXEC Mode. The user needs to further use the **enable** command to enter the Privileged EXEC Mode.

When the user login with a Level higher than or equal to 2, the user will directly enter the Privileged EXEC Mode. Therefore, the Privileged EXEC Mode can be in Levels 2 to 15.

The user can specify the password in the encrypted form or in the plain-text form. If it is in the plain-text form, but the service password encryption is enabled, then the password will be converted to the encrypted form.

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

By default, the user account is empty. When the user account is empty, the user will be directly in the User EXEC Mode at Level 1. The user can further enter the Privileged EXEC Mode using the **enable** command.

Example

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

```
Switch# configure terminal
Switch(config)# username admin privilege 15 password 0 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)#
```

5-23 password

This command is used to create a new password. Use the **no** form of the command to remove the password.

password [0 | 7] *PASSWORD*

no password

Parameters

0	Specifies the password in clear, plain text. The password length is between 1 and 32 characters and can contain embedded spaces. It is case-sensitive. If the password syntax cannot be specified, the syntax remains plain text.
7	Specifies the encrypted password based on SHA-1. The password length is fixed at 35 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text.
PASSWORD	Specifies the password for the user.

Default

None.

Command Mode

Line Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to create a new user password. Only one password can be used for each type of line.

Example

This example shows how to create a password for the console line.

```
Switch# configure terminal
Switch(config)# line console
Switch(config-line)# password 123
Switch(config-line)#
```

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 the 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-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 number of interfaces or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

By default, no entries exist.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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'.

Only physical ports and port channel interfaces are valid interface to be specified.

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 at port eth2/0/10 and port channel 3.

```
Switch#configure terminal
```

```
Switch(config)# ip arp spoofing-prevention 10.254.254.251 00-00-00-11-11-11 interface
eth2/0/10
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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 eth2/0/10

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. Authentication, Authorization, and Accounting (AAA) Commands

7-1 aaa accounting commands

This command is used to configure the accounting method list used for all commands at the specified privilege level. Use the **no** command to remove an accounting method list.

aaa accounting commands *LEVEL* **{default |** *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***...]**

no aaa accounting commands *LEVEL* **{default |** *LIST-NAME***}**

Parameters

LEVEL	Specifies to do accounting for all configure commands at the specified privilege level. Valid privilege level entries are 1 to 15.
default	Specifies to configure the default method list for accounting.
LIST-NAME	Specifies the name of the method list. This name can be up to 32 characters long.
METHOD1 **[***METHOD2***...]**	Specifies the list of methods that the accounting 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. **group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command. **group** *GROUP-NAME* – Specifies to use the server groups defined by the **aaa group server tacacs+** command. **none** – Specifies no to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the method list for accounting of commands.

Example

This example shows how to create a method list for accounting of the privilege level of 15 using TACACS+ and sends the accounting messages at the start and end time of access.

```
Switch#configure terminal
Switch(config)#aaa accounting commands 15 list-1 start-stop group tacacs+
```

7-2 aaa accounting exec

This command is used to configure the method list used for EXEC accounting for a specific line. Use the **no** form of the command to disable the accounting EXEC.

aaa accounting exec {default | *LIST-NAME***} start-stop** *METHOD1* **[***METHOD2***...]**

no aaa accounting exec {default | *LIST-NAME***}**

Parameters

default	Specifies to configure the default method list for EXEC accounting.
LIST-NAME	Specifies the name of the method list. This name can be up to 32 characters long.
METHOD1 [METHOD2...]	Specifies the list of methods that the accounting 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. **group radius** – Specifies to use the servers defined by the RADIUS server host command. **group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command. **group** *GROUP-NAME* – Specifies to use the server groups defined by the AAA group server command. **none** – Specifies not to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the method list for EXEC accounting.

Example

This example shows how to create a method list for accounting of user activities using RADIUS, which will send accounting messages at the start and end time of access.

```
Switch#configure terminal
Switch(config)#aaa accounting exec list-1 start-stop group radius
```

7-3 aaa accounting network

This command is used to account user activity in accessing the network. Use the **no** command to remove the accounting method list.

aaa accounting network default start-stop *METHOD1* **[***METHOD2***...]**

no aaa accounting network default

Parameters

network	Specifies to perform accounting of network related service requests.
start-stop	Specifies to send accounting messages at both the start time and the end time of access. Users are allowed of access the network regardless of whether the start accounting message enables the accounting successfully.
default	Specifies to configure the default method list for network accounting.
METHOD1 **[***METHOD2***...]**	Specifies the list of methods that the accounting 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. **group radius** – Specifies to use the servers defined by the RADIUS server host command. **group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command. **group** *GROUP-NAME* – Specifies to use the server groups defined by the AAA group server command. **none** – Specifies no to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the accounting method list for network access fees. For the default method list to take effect, enable AAA first by using the **aaa new-model** command. The accounting system is disabled if the default method list is not configured.

Example

This example shows how to enable accounting of the network access fees using RADIUS and sends the accounting messages at the start and end time of access:

```
Switch#configure terminal
Switch(config)#aaa accounting network default start-stop group radius
```

7-4 aaa accounting system

This command is used to account system events. Use the **no** command to remove the accounting method list.

aaa accounting system default start-stop *METHOD1* **[***METHOD2***...]**

no aaa accounting system default

Parameters

system	Specifies to perform accounting for system-level events.
start-stop	Specifies to send accounting messages at both the start time and the end time of access. Users are allowed to access the network regardless of whether the start accounting message enables the accounting successfully.
default	Specifies to configure the default method list for system accounting.
METHOD1 **[***METHOD2***...]**	Specifies the list of methods that the accounting 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. **group radius** – Specifies to use the servers defined by the RADIUS server host command. **group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command. **group** *GROUP-NAME* – Specifies to use the server groups defined by the AAA group server command. **none** – Specifies no to perform accounting.

Default

No AAA accounting method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the accounting method list for system-events such as reboot, reset events. For the default method list to take effect, enable AAA first by using the **aaa new-model** command. The accounting system is disabled if the default method list is not configured.

Example

This example shows how to enable accounting of the system events using RADIUS and sends the accounting messages while system event occurs:

```
Switch#configure terminal
Switch(config)# aaa accounting system default start-stop group radius
```

7-5 aaa authentication enable

This command is used to configure the default method list used for determining access to the privileged EXEC level. Use the **no** command to remove the default method list.

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

no aaa authentication enable 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. **enable** – Specifies to use the local enable password for authentication. **group radius** – Specifies to use the servers defined by the RADIUS server host command. **group tacacs+** - Specifies to use the servers defined by the TACACS+ server host command. **group** *GROUP-NAME* – Specifies to use the server groups defined by the AAA group server command. **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 authentication method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the default authentication method list for determining access to the privileged EXEC level when users issue the **enable [privilege LEVEL]** command. The authentication with the RADIUS server will be based on the privilege level and take either “enable12” or “enable15” as the user name.

Example

This example shows how to set the default method list for authenticating. The method tries the server group “group2”.

```
Switch#configure terminal
Switch(config)# aaa authentication enable default group group2
```

7-6 aaa authentication dot1x

This command is used to configure the default method list used for 802.1X authentication. Use the **no** 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 authentication if it is not denied by previous method authentication.

Default

No AAA authentication method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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
```

7-7 aaa authentication login

This command is used to configure the method list used for login authentication. Use the **no** command to remove a login method list.

aaa authentication login {default | *LIST-NAME***}** *METHOD1* **[***METHOD2***...]**

no aaa authentication login {default | *LIST-NAME***}**

Parameters

default	Specifies to configure the default method list for login authentication.
LIST-NAME	Specifies the name of the method list other than the default method list. This name can be up to 32 characters long.
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 tacacs+** - Specifies to use the servers defined by the TACACS+ server host command. **group** *GROUP-NAME* – Specifies to use the server groups defined by the AAA group server command. **none** - Normally, the method is listed as the last method. The user will

	pass authentication if it is not denied by previous method's authentication.

Default

No AAA authentication method list is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the authentication method list used for login authentication. Multiple method lists can be configured. The default keyword is used to define the default method list.

If authentication uses the default method list but the default method list does not exist, then the authentication will be performed via the local database.

The login authentication authenticates the login user name and password, and also assigns the privilege level to the user based on the database.

A method list is a sequential list describing the authentication methods to be queried in order to authenticate a user. Method lists enable you to designate one or more security protocols to be used for authentication, thus ensuring a backup system for authentication in case the initial method fails. The switch system uses the first listed method to authenticate users. If that method fails to respond, the switch system selects the next authentication method listed in the method list. This process continues until there is successful communication with a listed authentication method or all methods defined in the method list are exhausted.

It is important to note that the switch system attempts authentication with the next listed authentication method only when there is no response from the previous method. If authentication fails at any point in this cycle, meaning that the security server or local username database responds by denying the user access, the authentication process stops and no other authentication methods are attempted.

Example

This example shows how to set the default login methods list for authenticating of login attempts.

```
Switch#configure terminal
Switch(config)# aaa authentication login default group group2 local
```

7-8 aaa authentication mac-auth

This command is used to configure the default method list used for MAC authentication. Use the **no** command to remove the default method list.

aaa authentication mac-auth default *METHOD1* **[***METHOD2***...]**

no aaa authentication mac-auth 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 authentication if it is not denied by previous method authentication.

Default

No AAA authentication method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

This example shows how to set the default methods list for authenticating mac-auth users.

```
Switch#configure terminal
Switch(config)# aaa authentication mac-auth default group radius
```

7-9 aaa authentication web-auth

This command is used to configure the default method list used for Web authentication. Use the **no** command to remove the default method list.

aaa authentication web-auth default *METHOD1* **[***METHOD2***...]**

no aaa authentication web-auth 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 authentication if it is not denied by previous method authentication.

Default

No AAA authentication method is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the default authentication method list for Web authentication. Initially, the default method list is not configured. The authentication of the web-auth request will be performed based on the local database.

Example

This example shows how to set the default method list for authenticating web-auth users.

```
Switch#configure terminal
Switch(config)# aaa authentication web-auth default group radius
```

7-10 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 the 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 that does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to define a RADIUS server group. The created server group is used in the definition of method lists used for authentication, or accounting by using AAA authentication and AAA accounting 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)# exit
Switch(config)#
```

7-11 aaa group server tacacs+

This command is used to enter the TACACS+ group server configuration mode to associate server hosts with the group. Use the **no** form of the command to remove a TACACS+ server group

aaa group server tacacs+ *GROUP-NAME*

no aaa group server tacacs+ *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 that does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to enter the TACACS+ group server configuration mode. Use the server command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting by using the AAA authentication and AAA accounting command.

Example

This example shows how to create a TACACS+ server group with two entries.

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

7-12 aaa new-model

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

Command Default Level

Level: 15.

Usage Guideline

The user should use the **aaa new-model** command to enable AAA before the authentication and accounting via the AAA method lists take effect. If AAA is disabled, the login user will be authenticated via the local user account table created by the username command. The enable password will be authenticated via the local table which is defined via the enable password command.

Example

This example shows how to enable the AAA function.

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

7-13 accounting commands

This command is used to configure the method list used for command accounting via a specific line. Use the **no** form of the command to disable do accounting command.

accounting commands *LEVEL* **{default |** *METHOD-LIST***}**

no accounting commands *LEVEL*

Parameters

LEVEL	Specifies to do accounting for all **configure** commands at the specified privilege level. Valid privilege level entries are 1 to 15.
default	Specifies to do accounting based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this option is disabled.

Command Mode

Line Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting commands** command. If the method list does not exist, the command does not take effect. The user can specify different method lists to account commands at different levels. A level can only have one method list specified.

Example

This example shows how to enable the command accounting level 15 configure command issued via the console using the accounting method list named “cmd-15” on the console.

```
Switch# configure terminal
Switch(config)# aaa accounting commands 15 cmd-15 start-stop group tacacs+
Switch(config)# line console
Switch(config-line)# accounting commands 15 cmd-15
Switch(config-line)#
```

7-14 accounting exec

This command is used to configure the method list used for EXEC accounting for a specific line. Use the **no** form of the command to disable the accounting EXEC option.

accounting exec {default | *METHOD-LIST***}**

no accounting exec

Parameters

default	Specifies to use the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting exec** command. If the method list does not exist, the command does not take effect.

Example

This example shows how to configure the EXEC accounting method list with the name of “list-1”. It uses the RADIUS server. If the security server does not response, it does not perform accounting. After the configuration, the EXEC accounting is applied to the console.

```
Switch#configure terminal
Switch(config)# aaa accounting exec list-1 start-stop group radius
switch(config)# line console
switch(config-line)# accounting exec list-1
```

7-15 clear aaa counters servers

This command is used to clear the authentication and accounting (AAA) server statistic counters.

clear aaa counters servers {all | radius {*IP-ADDRESS***| *IPV6-ADDRESS* | all} | tacacs {***IP-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.
tacacs *IP-ADDRESS*	Specifies to clear server counter information related to a TACACS IPv4 host.
tacacs all	Specifies to clear server counter information related to all TACACS hosts.
sg *NAME*	Specifies to clear server counter information related to all hosts in a server group.

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 15.

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#
```

7-16 ip http authentication aaa login-authentication

This command is used to specify an AAA authentication method list for the authentication of the HTTP server users. Use the **no** form of the command to reset to use the default method list.

ip http authentication aaa login-authentication {default | *METHOD-LIST***}**

no ip http authentication aaa login-authentication

Parameters

default	Specifies to authenticate based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this **default** option is used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

For authentication via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa authentication login** command. If the method list does not exist, the command does not take effect, and the authentication will be done via the default login method list.

Example

This example shows how to configure HTTP sessions to use the method list “WEB-METHOD” for login authentication.

```
Switch# configure terminal
Switch(config)# aaa authentication login WEB-METHOD group group2 local
Switch(config)# ip http authentication aaa login-authentication WEB-METHOD
Switch(config)#
```

7-17 ip http accounting exec

This command is used to specify an AAA accounting method for HTTP server users. Use the **no** form of the command to reset to the default setting.

ip http accounting exec {default | *METHOD-LIST***}**

no ip http accounting exec

Parameters

default	Specifies to do accounting based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

For accounting via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa accounting exec** command. If the method list does not exist, the command does not take effect.

Example

This example shows how to specify that the method configured for AAA should be used for accounting for HTTP server users. The AAA accounting method is configured as the RADIUS accounting method.

```
Switch# configure terminal
Switch(config)# aaa accounting exec list-1 start-stop group radius
Switch(config)# ip http accounting exec list-1
Switch(config)#
```

7-18 ip radius source-interface

This command is used to specify the interface whose IP address will be used as the source IP address for sending RADIUS packets. To revert back to the default setting, use the **no** form of this command.

ip radius source-interface *INTERFACE-ID*

no ip radius source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source IP address for sending RADIUS packets.

Default

The IP address of the closest interface will be used.

Command Mode

Global Configuration Mode or Server Group Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command can be used to specify the interface whose IP address will be used as the source IP address for sending RADIUS packets. If the source interface is specified in both the global configuration mode and group server configuration mode, the source interface specified in group server configuration mode take precedence.

When the server is located on the Out-Of-Band Management Port, the user should specify the interface ID of Out-Of-Band Management Port as the source interface in order to send the request packet to the management port

Example

This example shows how to set VLAN100, whose IP address will be used as the source IP address, for sending RADIUS packets.

```
Switch#configure terminal
Switch(config)# ip radius source-interface vlan100
```

7-19 ip tacacs source-interface

This command is used to specify the interface whose IP address will be used as the source IP address for sending TACACS packets. To revert to the default setting, use the **no** form of this command.

ip tacacs source-interface *INTERFACE-ID*

no ip tacacs source-interface

Parameters

INTERFACE_ID	Specifies the interface whose IP address will be used as the source IP address for sending TACACS packets.

Default

The IP address of the closest interface will be used.

Command Mode

Global Configuration Mode or Server Group Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command can be used to specify the interface whose IP address will be used as the source IP address for sending TACACS packets. If the source interface is specified in both the global configuration mode and group server configuration mode, the source interface specified in group server configuration mode take precedence.

When the server is located at the Out-Of-Band Management Port, the user should specify the interface ID of Out-Of-Band Management Port as the source interface in order to send the request packet to the management port

Example

This example shows how to set VLAN100, whose IP address will be used as the source IP address, for sending TACACS packets.

```
Switch#configure terminal
Switch(config)# ip tacacs source-interface vlan100
```

7-20 ip vrf forwarding (server-group)

This command is used to configure the VRF reference of an authentication, authorization, and accounting (AAA) RADIUS or TACACS+ server group, use the **ip vrf forwarding** command in the server group configuration mode. To enable server groups to use the global (default) routing table, use the **no** form of this command.

ip vrf forwarding *VRF-NAME*

no ip vrf forwarding

Parameters

VRF-NAME	Specifies the name of the Virtual Routing and Forwarding (VRF) entry.

Default

Server groups use the global routing table.

Command Mode

Server Group Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to specify a VRF for an AAA RADIUS or TACACS+ server group. This command enables access users to utilize AAA servers in different routing domains.

Example

This example shows how to specify the VRF for a RADIUS server group.

```
Switch#configure terminal
Switch(config)#aaa group server radius _global
Switch(config-sg-radius)#server 172.16.10.254
Switch(config-sg-radius)#exit
Switch(config)#
Switch(config)#aaa group server radius _sales
Switch(config-sg-radius)#server 10.10.0.1
Switch(config-sg-radius)#ip vrf forwarding sales
Switch(config-sg-radius)#exit
Switch(config)#
```

7-21 ipv6 radius source-interface

This command is used to specify the interface whose IPv6 address will be used as the source IPv6 address for sending RADIUS packets. To revert back to the default setting, use the **no** form of this command.

ipv6 radius source-interface *INTERFACE-ID*

no ipv6 radius source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IPv6 address will be used as the source IPv6 address for sending RADIUS packets.

Default

The IPv6 address of the closest interface will be used.

Command Mode

Global Configuration Mode or Server Group Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to specify the interface whose IPv6 address will be used as the source IPv6 address for sending RADIUS packets. If the source interface is specified in both the global configuration mode and group server configuration mode, the source interface specified in group server configuration mode take precedence.

When the server is located at the Out-Of-Band Management Port, the user should specify the interface ID of Out-Of-Band Management Port as the source interface in order to send the request packet to the management port.

Example

This example shows how to set VLAN100, whose IPv6 address will be used as the source IPv6 address, for sending RADIUS packets.

```
Switch#configure terminal
Switch(config)# ipv6 radius source-interface vlan100
```

7-22 login authentication

This command is used to configure the method list used for login authentication via a specific line. Use the **no** form of the command to reset back to the default method list.

login authentication {default | *METHOD-LIST***}**

no login authentication

Parameters

default	Specifies to authenticate based on the default method list.
METHOD-LIST	Specifies the name of the method list to use.

Default

By default, the default method list is used.

Command Mode

Line Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

For authentication via the method list to take effect, enable AAA first by using the **aaa new-model** command. Create the method list first by using the **aaa authentication login** command. If the method list does not exist, the command does not take effect and the authentication will be done via the default login method list.

When **aaa new-model** is enabled, the default method list is used for authentication.

Example

This example shows how to set the local console line to use the method list “CONSOLE-LINE-METHOD” for login authentication.

```
Switch#configure terminal
Switch(config)# aaa authentication login CONSOLE-LINE-METHOD group group2 local
Switch(config)# line console
Switch(config-line)# login authentication CONSOLE-LINE-METHOD
Switch(config-line)#
```

7-23 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 the command to revert back 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.

Command Default Level

Level: 15.

Usage Guideline

This command can be used 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
```

7-24 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***] [acct-port** *PORT***] [timeout** *SECONDS***] [retransmit** *COUNT***] key [0 | 7]** *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-NUMBER*	(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.
acct-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending accounting packets. The range is 0 to 65535. Set the port number to zero if the server host is not for accounting purposes. The default value is 1813.
timeout *SECONDS*	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
0	(Optional) Specifies the password in clear text form. This is the default option.
7	(Optional) Specifies the password in the encrypted form.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can between 1 and 32 clear text characters.

Default

By default, no server is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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 acct-port 1501 timeout
8 retransmit 3 key ABCDE
Switch(config)# radius-server host 172.19.10.101 auth-port 1600 acct-port 1601 timeout
3 retransmit 1 key ABCDE
```

7-25 server (RADIUS)

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

Command Default Level

Level: 15.

Usage Guideline

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. The defined server group can be specified as the method list for authentication, or accounting via the AAA authentication and AAA accounting 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)# exit
Switch(config)#
```

7-26 server (TACACS+)

This command is used to associate a TACACS+ server with a server group. Use the **no** form of the command to remove a server from the server group.

server *IP-ADDRESS*

no server *IP-ADDRESS*

Parameters

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

Default

By default, no host is in the server group.

Command Mode

TACACS+ Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use the **aaa group server tacacs+** command to enter the TACACS+ group server configuration mode. Use the **server** command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** command. The configured servers in the group will be attempted in the configured order. Use the **tacacs-server host** command to create a server host entry. A host entry is identified by the IP Address.

Example

This example shows how to create two TACACS+ server hosts. A server group is then created with the two server hosts.

```
Switch#configure terminal
Switch(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
Switch(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
Switch(config)#aaa group server tacacs+ group2
Switch(config-sg-tacacs+)# server 172.19.10.100
Switch(config-sg-tacacs+)# server 172.19.122.3
Switch(config-sg-tacacs+)# exit
Switch(config)#
```

7-27 show aaa

This command is used to display the AAA global state.

show aaa

Parameters

None.

Default

None.

Command Mode

Privilege User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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#
```

7-28 tacacs-server host

This command is used to create a TACACS+ server host. Use the **no** form of this command to remove a server host.

tacacs-server host *IP-ADDRESS* **[port** *PORT***] [timeout** *SECONDS***] key [0 | 7]** *KEY-STRING*

no tacacs-server host *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IP address *of* the TACACS+ server.
port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending request packets. The default port number is 49. The range is 1 to 65535.
timeout *SECONDS*	(Optional) Specifies the time-out value. This value must be between 1 and 255 seconds. The default value is 5 seconds.
0	(Optional) Specifies the password in the clear text form. This is the default option.
7	(Optional) Specifies the password in the encrypted form.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can be from 1 to 254 clear text characters.

Default

No TACACS+ server host is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use the **tacacs-server host** command to create TACACS+ server hosts before it can be associated with the TACACS+ server group using the **server** command.

Example

This example shows how to create two TACACS+ server hosts with the different IP addresses.

```
Switch#configure terminal
Switch(config)# tacacs-server host 172.19.10.100 port 1500 timeout 8 key ABCDE
Switch(config)# tacacs-server host 172.19.122.3 port 1600 timeout 3 key ABCDE
Switch(config)#
```

7-29 show radius statistics

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

show radius statistics

Parameters

None.

Default

None.

Command Mode

Privilege User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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: 172.19.192.80: Auth-Port 1645, Acct-Port 1646
State is UP
                                Auth.   Acct.
Round Trip Time:                10      10
Access Requests:                 4      NA
Access Accepts:                  0      NA
Access Rejects:                  4      NA
Access Challenges:               0      NA
Acct Request:                   NA       3
Acct Response:                  NA       3
Retransmissions:                 0       0
Malformed Responses:             0       0
Bad Authenticators:              0       0
 Pending Requests:               0       0
 Timeouts:                       0       0
 Unknown Types:                  0       0
 Packets Dropped:                0       0
```

Display Parameters

Auth.	Statistics for authentication packets.
Acct.	Statistics for accounting 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.
Acct Request	The number of RADIUS Accounting-Request packets sent. This does not include retransmissions.
Acct Response	The number of RADIUS packets received on the accounting port 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.

7-30 show tacacs statistics

This command is used to display the interoperation condition with each TACACS+ server.

show tacacs statistics

Parameters

None.

Default

None.

Command Mode

Privilege EXEC Mode or and configuration mode.

Command Default Level

Level: 1.

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 tacacs statistics
TACACS+ Server: 172.19.192.80/49, State is UP
Socket Opens: 0
Socket Closes: 0
Total Packets Sent: 0
Total Packets Recv: 0
Reference Count: 0
```

Display Parameters

TACACS+ Server	IP address of the TACACS+ server.
Socket Opens	Number of successful TCP socket connections to the TACACS+ server.
Socket Closes	Number of successfully closed TCP socket attempts.
Total Packets Sent	Number of packets sent to the TACACS+ server.
Total Packets Recv	Number of packets received from the TACACS+ server.
Reference Count	Number of authentication requests from the TACACS+ server.

8. Basic IPv4 Commands

8-1 arp

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

arp [vrf *VRF-NAME***]** *IP-ADDRESS HARDWARE-ADDRESS*

no arp [vrf *VRF-NAME***]** *IP-ADDRESS HARDWARE-ADDRESS*

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.
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.

Command Default Level

Level: 12.

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
```

8-2 arp timeout

This command is used to set the ARP aging time for the ARP table. Use the **no** command to revert to 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.

Default

The default value is 240 minutes.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Used to set the ARP aging time for the ARP table. Use the **no** command to revert to default setting.

Example

This example shows how to set the ARP timeout to 60 minutes to allow entries to time out more quickly than the default setting.

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

8-3 clear arp-cache

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

clear arp-cache [vrf *VRF-NAME***] {all | interface** *INTERFACE-ID* **|** *IP-ADDRESS***}**

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.
all	Specifies to clear the dynamic ARP cache entries associated with all interfaces.
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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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#
```

8-4 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** command to remove the configuration of an IP address or disable DHCP on the interface.

ip address {*IP-ADDRESS SUBNET-MASK* **[secondary] | 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.
secondary	(Optional) Specifies that the configured address is a secondary IP address. If this keyword is not specified, the configured address is the primary 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.

Command Default Level

Level: 12.

Usage Guideline

The IPv4 address of an interface can be either manually assigned by the user or dynamically assigned by the DHCP server. For manual assignment, the user can assign multiple networks to a VLAN, each with an IP address. Among these multiple IP addresses, one of them must be the primary IP address and the rest are secondary IP address. The primary address will be used as the source IP address for SNMP trap messages or SYSLOG messages that are sent out from the interface. Use the **no ip address** command to delete the configured IP address entry.

Example

This example shows how to set 10.108.1.27 is the primary address and 192.31.7.17 and 192.31.8.17 are secondary addresses for VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip address 10.108.1.27 255.255.255.0
Switch(config-if)# ip address 192.31.7.17 255.255.255.0 secondary
Switch(config-if)# ip address 192.31.8.17 255.255.255.0 secondary
Switch(config-if)#
```

8-5 ip proxy-arp

This command is used to enable the proxy ARP option for an interface. Use the **no** command to revert to the default setting.

ip proxy-arp

no ip proxy-arp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the proxy ARP state for an interface. When proxy ARP is enabled, the system will respond to ARP requests for IP addresses within the local connected subnets. Proxy ARP can be used in the network where hosts have no default gateway configured.

Example

This example shows how to enable proxy the ARP feature on the interface of VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip proxy-arp
Switch(config-if)#
```

8-6 ip local-proxy-arp

This command is used to enable the local proxy ARP feature on an interface. Use the **no** form of the command to revert to the default setting.

ip local-proxy-arp

no ip local-proxy-arp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12,15.

Usage Guideline

Use this command to enable the local proxy ARP function on an interface. This command is used in the primary VLAN of a private VLAN domain to enable routing of packets among secondary VLANs or isolated ports within the domain. The command only take effects when **ip proxy arp** is enabled.

Example

This example shows how to enable local proxy ARP on VLAN100.

```
Switch# configure terminal
Switch(config)# interface vlan100
switch(config-if)# ip local-proxy-arp
switch(config-if)#
```

8-7 ip mtu

This command is used to set the MTU value. Use the **no** form to revert to the default setting.

ip mtu *BYTES*

no ip mtu

Parameters

BYTES	Specifies to set the IP MTU value. The range is 512 to 16383 bytes.

Default

By default, the MTU value is 1500 bytes.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Some routing protocols, such as OSPF, will advertise this setting in the routing updates.

Example

This example shows how to set the IP MTU value as 6000 bytes for VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if) ip mtu 6000
Switch(config-if)# exit
Switch(config)#
```

8-8 show arp

This command is used to display the Address Resolution Protocol (ARP) cache.

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

Parameters

VRF-NAME	(Optional) Specifies the VRF instance name.
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 network.
HARDWARE-ADDRESS	(Optional) Specifies to display ARP entries whose hardware address equal to this address

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Used 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 10.108.42.112           00-00-a7-10-4b-af   vlan100          forever
10.108.42.114             00-00-a7-10-85-9b   vlan200          forever
10.108.42.121             00-00-a7-10-68-cd   vlan300          125

Total Entries: 3

Switch#
```

8-9 show arp timeout

This command is used to display the aging time of Address Resolution Protocol (ARP) cache.

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

Parameters

INTERFACE-ID	Specifies the interface ID.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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)
---------------------------------------
vlan100                30
vlan200                40

Total Entries: 2

Switch#
```

8-10 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

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
vlan2               20.1.1.1        up

Total Entries: 2

Switch#
```

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

```
Switch# show ip interface vlan1

Interface Vlan1 is enabled, link status is up,
   VRF Name is vpn-a
IP address is 10.0.0.4/24 (Manual)
ARP timeout is 240 minutes
IP MTU is 1500 bytes
Helper Address is not set
Proxy ARP is enabled
IP Local Proxy ARP is disabled.
IP Directed Broadcast is disabled
gratuitous-send is enabled, interval is 30 seconds

Switch#
```

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

```
Switch# show ip interface loopback1

Interface Loopback1 is enabled, link status is up,
IP address is 10.0.0.4/24

Switch#
```

8-11 ip directed-broadcast

This command is used to enable the conversion of IP directed broadcasts received by the interface to physical broadcasts when the destination network is directly connected to the switch. Use the **no** command to disable the conversion.

ip directed-broadcast

no ip directed-broadcast

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the IP directed broadcast state for an interface. This command does not affect unicast routing of the IP directed broadcast, forwarding of the IP directed broadcast packet whose destination networks are not subnets local to the switch.

This command only affects the forwarding of IP directed broadcast packets whose destination networks are subnets local to the switch. If the IP directed broadcast option is enabled, then these packets are translated to broadcast and forwarded to all the hosts in the destination subnet. The forwarded interface can be the receiving interface or other interfaces of the switch.

Example

This example shows how to enable the IP directed broadcast feature on the interface of VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip directed-broadcast
Switch(config-if)# exit
Switch(config)#
```

9. Basic IPv6 Commands

9-1 clear ipv6 neighbors

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

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

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command will only clear dynamic neighbor cache entries.

Example

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

```
Switch# enable
Switch# clear ipv6 neighbors vlan1
Switch#
```

9-2 ipv6 address

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

ipv6 address {*IPV6-ADDRESS***|***PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS***|***PREFIX-LENGTH* **|** *IPV6-ADDRESS* **link-local}**

no ipv6 address {*IPV6-ADDRESS***|***PREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITS***|***PREFIX-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.

PREFIX-NAME	Specifies the name of the prefix with a maximum of 32 characters. The syntax allows characters for general strings, but does not allow spaces.
SUB-BITS	Specifies the sub-prefix part and host part of the IPv6 address.
link-local	Specifies a link-local address to be configured.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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.

An interface can have multiple IPv6 addresses assigned using a variety of mechanisms, including manual configuration, stateless address configuration, and stateful address configuration. However, within the same prefix, only one IPv6 address can be configured.

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
```

This example shows how to configure an IPv6 address based on a general prefix obtained by the DHCPv6 client. The global address will be configured after the general prefix is obtained via the DHCPv6 client. Suppose the obtained general prefix is 2001:2:3/48 and the final constructed IPv6 address is 2001:2:3:4:5::3/64.

```
Switch# configure terminal
Switch(config)# interface vlan2
Switch(config-if)# ipv6 address dhcp-prefix  1:2:3:4:5::3/64
```

This example shows how to remove a generation of IPv6 address based on the DHCPv6 obtained prefix.

```
Switch# configure terminal
Switch(config)# interface vlan2
```

```
Switch(config-if)# no ipv6 address dhcp-prefix 0:0:0:2::3/64
```

9-3 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 the 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, the default keyword causes a default route to be installed using that default router. The default keyword can be specified only on one interface.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only available for the VLAN IPv6 interface (IPv6 is enabled on the VLAN interface). By default the auto-configuration option is disabled.

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 option 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+. The static default route has higher route preference than the default route of the SLAAC type.

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)#
```

9-4 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 the 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.

Command Default Level

Level: 12.

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)#
```

9-5 ipv6 address dhcp

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

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Parameters

rapid-commit	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

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the interface to use DHCPv6 to get an IPv6 address. When the **no ipv6 address dhcp** command is used, the previous DHCPv6 obtained IP address will be removed. If the **rapid commit** keyword is specified for the command, the rapid commit option will be included in the solicit message to request for the two-message exchange for address delegation.

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)#
```

9-6 ipv6 enable

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

Command Default Level

Level: 12.

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)#
```

9-7 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 range. Using the value 0 means to use the default value to send packets. The valid range is 0 to 255.

Default

The default value is 64.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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.

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

9-8 ipv6 mtu

This command is used to configure the MTU value for IPv6. Use the **no** form to revert to the default setting.

ipv6 mtu *BYTES*

no ipv6 mtu

Parameters

BYTES	Specifies to set the IPv6 MTU value. The range is 1280 to 65534 bytes.

Default

By default, the IPv6 MTU value is 1500 bytes.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for Layer 3 capable interface configuration. Use this command to configure the MTU to be advertised in RA messages. The IPv6 packet originated at the system will be transmitted based on this value. The check is done in the egress direction. Oversized packets will be sent to the supervisor blade for further processing.

Example

This example shows how to set the IPv6 MTU value as 6000 bytes at VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if) ipv6 mtu 6000
Switch(config-if)# exit
Switch(config)#
```

This example shows how to restore the default IPv6 MTU value.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if)# no ipv6 mtu
Switch(config-if)#
```

9-9 ipv6 nd managed-config-flag

This command is used to turn on the management configuration flag in the advertised RA message. Use the **no** form of the command to turn off the 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.

Command Default Level

Level: 12.

Usage Guideline

When the neighbor host receives the RA which has flag turned on, the host should use a stateful configuration protocol to obtain IPv6 addresses.

Example

This example shows how to turn on 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)#
```

9-10 ipv6 nd other-config-flag

This command is used to turn on the other configuration flag in the advertised RA message. Use the **no** form of the command to turn off the 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.

Command Default Level

Level: 12.

Usage Guideline

By setting the other configuration flag on, the router instructs the connected hosts to use a stateful configuration protocol to obtain auto-configuration information other than the IPv6 address.

Example

This example shows how to turn on the other configuration flag.

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

9-11 ipv6 nd prefix

This command is used to configure an IPv6 prefix to be advertised in RA messages. Use the **no** form of the 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/PREFIX-LENGTH	Specifies the IPv6 prefix to be created or advertised in the RA on the interface.
VALID-LIFETIME	(Optional) Specifies the valid lifetime in seconds. This value must be between 0 and 4294967295. If not specified, the default valid lifetime value is 2592000 seconds (30 days).
PREFERRED-LIFETIME	(Optional) Specifies the preferred lifetime in seconds. This value must be between 0 and 4294967295. If not specified, the default preferred lifetime value is 604,800 seconds (7 days)
off-link	(Optional) Specifies to turn off the on-link flag. If not specified, the default off-link flag is ON.
no-autoconfig	(Optional) Specifies to turn off the auto-configure flag. If not specified, the default auto-configure flag is ON

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The status of a prefix can be in one of the following combinations:

- Combination 1:Both the off-link and no-autoconfig options are not specified.
  - The prefix is inserted in the routing table. L bit = 1, A bit = 1.
- Combination 2: The no-autoconfig option is specified.
  - The prefix is inserted in the routing table. L bit = 1, A bit = 0.
- Combination 3: The off-link option is specified.
  - The prefix is not inserted in the routing table. L bit = 0, A bit = 1.

For a prefix, the valid lifetime should be greater than the preferred lifetime. They are meaningful for a prefix that has the A bit ON. The received host will do the stateless address configuration based on the prefix. If the lifetime of a prefix has exceeded the preferred life time, 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.

Example

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

9-12 ipv6 nd ra interval

This command is used to configure the IPv6 RA interval for an interface. Use the **no** form of the command to reset the RA interval 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

The default maximum interval is 200 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The minimum interval time will never be less than 3 seconds.

Example

This example shows how to configure the IPv6 RA interval timer value.

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

9-13 ipv6 nd ra lifetime

This command is used to specify the lifetime value in the advertised RA. Use the **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

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

Example

This example shows how to specify the lifetime value in the advertised RA.

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

9-14 ipv6 nd suppress-ra

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

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameters

None.

Default

RA is not disabled on the VLAN interface.

RA is disabled on the tunnel interface.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **ipv6 nd suppress-ra** command to disable sending of RA messages on the interface. Use the **no ipv6 nd suppress-ra** command to re-enable sending of RA messages on the ISATAP tunnel 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)#
```

9-15 ipv6 nd reachable-time

This command is used to configure the reachable time used in the ND protocol. Use the **no** form of the 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. This value must be between 0 and 3600000 milliseconds, in multiples of 1000.

Default

The default value advertised in RA is 1200000.

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

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The configured time is used by the router on the interface and is also advertised in the RA message. If the specified time is 0, the router will use 1200 seconds on the interface and advertise 1200 (unspecified) in the RA message. The reachable time is used by the IPv6 node in determining the reachability of the neighbor 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)#
```

9-16 ipv6 nd ns-interval

This command is used to specify the interval between retransmissions of NS messages. Use the **no** form of the 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

	in milliseconds. This value must be between 0 and 3600000 milliseconds, in multiples of 1000.

Default

The default value advertised in RA is 0.

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

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The configured time is used by the router on the interface and is also advertised in the 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)#
```

9-17 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 for creating 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.

Command Default Level

Level: 12.

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)#
```

9-18 show ipv6 general-prefix

This command is used to display IPv6 general prefix information.

show ipv6 general-prefix [*PREFIX-NAME***]**

Parameters

PREFIX-NAME	(Optional) Specifies the name of the general prefix to be displayed. If the general prefix name is not specified, all general prefixes will be displayed. The general prefix name can be up to 32 characters.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information of IPv6 general prefixes.

Example

This example shows how to display all IPv6 general prefix on the system.

```
Switch# show ipv6 general-prefix

IPv6 prefix yy
 Acquired via DHCPv6 PD
   vlan1: 200::/48
       Valid lifetime 2592000, preferred lifetime 604800
   Apply to interfaces
     vlan2: ::2/64

Total Entries: 1

Switch#
```

9-19 show ipv6 interface

This command is used to display IPv6 interface information.

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

Parameters

INTERFACE-ID	(Optional) Specifies the interface for display.
brief	(Optional) Specifies to display brief information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IPv6 interface related configurations. For IPv6 tunnel interface, only the ISATAP tunnel will be displayed.

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::201:1FF:FE02:305
  Global unicast address:
      200::2/64 (DHCPv6 PD)
  IP MTU is 1500 bytes
  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

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#
```

9-20 show ipv6 neighbors

This command is used to display IPv6 neighbor information.

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

Parameters

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

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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.

10. Border Gateway Protocol (BGP) Commands

10-1 address-family ipv4 (BGP)

This command is used to enter the address family configuration mode to configure the setting specific to the address family. Use the **no** form of the command to revert the setting of the specified address family

address-family ipv4 [unicast | vrf *VRF-NAME***]**

no address-family ipv4 [unicast | vrf *VRF-NAME***]**

Parameters

unicast	(Optional) Specifies the IPv4 unicast address prefixes.
vrf *VRF-NAME*	Specifies the name of the VRF instance to enter IPv4 VRF address family configuration mode.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To specify the command setting specific to different address family, enter the address family configuration mode to configure the command.

For all command settings that are configured in the IPv4 unicast address family mode is equivalent to the command settings configured in the router configuration mode.

Use the **exit** command to leave the address family configuration mode and return to router configuration mode without removing the existing configuration.

Example

This example shows how to enter and exit the address family configuration mode for the IPv4 address family.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4
Switch(config-router-af)# exit
Switch(config-router)#
```

This example shows how to enter VRF address family and create a BGP peer.

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)# neighbor 5.5.5.5 remote-as 20
Switch(config-router-af)# exit
Switch(config-router)#
```

10-2 address-family vpnv4

This command is used to enter the IPv4 VPN address family mode. Use the **no** form of this command to delete the configuration of the VPNv4 address family.

address-family vpnv4

no address-family vpnv4

Parameters

None.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To specify the command setting specific to a different address family, enter the address family configuration mode to configure the command.

Use the **exit** command to leave the address family configuration mode and return to the router configuration mode without removing the existing configuration.

Example

This example shows how to enter the VPN4 address family and activate a BGP peer.

```
Switch# configure terminal
Switch(config)# router bgp 120
Switch(config-router)# address-family vpnv4
Switch(config-router-af)# neighbor 10.2.2.5 activate
Switch(config-router-af)# neighbor 10.2.2.5 send-community extended
Switch(config-router-af)# exit
Switch(config-router)#
```

10-3 aggregate-address

This command is used to create a BGP aggregated route. Use the **no** command to remove the aggregated route.

aggregate-address *NETWORK-NUMBERISUBNET-LENGTH* **[summary-only] [as-set]**

no aggregate-address *NETWORK-NUMBERISUBNET-LENGTH*

Parameters

NETWORK-NUMBER/ SUBNET-LENGTH	Specifies the network number and the length of the network that BGP will aggregate. The format of *NETWORK-NUMBER*/*SUBNET-LENGTH* can be 10.9.18.2/8.
summary-only	(Optional) Specifies to filter those routes that are more specific than the aggregated route.
as-set	(Optional) Specifies to generate autonomous system set path information.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 Unicast and VRF).

Command Default Level

Level: 12.

Usage Guideline

Route aggregation is a mechanism used to reduce the number of routing entries.

Use the aggregate command to create an aggregate entry. The aggregated route will be created in the routing table if there is any more specific route entry than the aggregated route and the characteristic of the aggregated route is the combined characteristic of the more specific routes. The aggregated route is sent as coming from the local AS. The atomic aggregation flag is set to indicate that the AS path information of the more specific route information might be lost from the aggregated entry.

If the summary-only option is not specified, the aggregated route, together with its more specific routes, is advertised. If specified, the more specific routes are not advertised.

When the as-set option is specified, the AS number information of those more-specific routes will be put in the AS set attribute of the aggregated route entry. An AS number is only listed once in the AS set even though it appear in the AS path of multiple paths. The atomic aggregator flag of the aggregated route entry is off to inform the neighbor that the AS path information of the aggregated path is not lost.

Example

This example shows how to propagate network 172.0.0.0 and suppresses the more specific route 172.10.0.0.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# aggregate-address 172.0.0.0/8 summary-only
```

10-4 bgp aggregate-next-hop-check

This command is used to enable the checking of the next hop of the BGP aggregated routes. Use the **no** form of this command to disable the BGP aggregate-next-hop-check.

bgp aggregate-next-hop-check

no bgp aggregate-next-hop-check

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable the checking of next hop of the BGP aggregated routes. Only the routes with the same next hop attribute can be aggregated if the BGP aggregate next hop check is enabled. Using the no form of this command is to disable the BGP aggregate-next-hop-check.

Example

This example shows how to configure the BGP aggregate-next-hop-check state.

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp aggregate-next-hop-check
```

10-5 bgp always-compare-med

This command is used to configure the Multi Exit Discriminator (MED) in best path selection for paths that are advertised from neighbors in either the same or different autonomous systems. Use the **no** command to use MED only for paths that are advertised from neighbors in the same autonomous system.

bgp always-compare-med

no bgp always-compare-med

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

MED is an attribute that is exchanged between of eBGP neighbors. MED is an attribute specified by a local peer, and advertised to the remote peer to affect the best path selection result in the remote peer. The remote peer will not pass the MED value with routes for further path advertisement. The lower MED value is preferred than the larger MED value.

By default, the MED attribute only affects the selection of paths that are advertised by the same AS. To use MED to further affects the selection of routes advertised from different AS, enable the always-compare-med command setting.

Example

This example shows how to apply the always-compare-med option to enable the comparison of the Multi Exit Discriminator (MED) for paths from neighbors in different autonomous systems.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp always-compare-med
```

10-6 bgp bestpath as-path ignore

This command is used to ignore the AS path as a discriminating factor in selection of the best path. Use the **no** command to restore using of the AS path in selection of the best path.

bgp bestpath as-path ignore

no bgp bestpath as-path ignore

Parameters

None.

Default

By default, the AS path is used in the selection of the best path.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The best path is selected based on the following algorithm. The paths are evaluated in sequence of the following rules.

- The path with the highest weight is preferred.
- The path with the highest local preference is preferred.
- The local routes generated by network command, redistribute command and aggregate command is preferred over other routes. The routes generated by network and redistribute command has higher preference than aggregate route.
- The path with shorter AS path is preferred.
- The origin attribute is compared. IGP is preferred over EGP, EGP is preferred over incomplete.
- The path with lower MED is preferred.
- The eBGP path is preferred over the iBGP path.
- The path which has the lowest IGP metric to the next hop is preferred.
- The path with the lowest router ID is preferred.
- When two paths are both external, the older path is preferred.
- Prefer the path from the neighbor with lowest IP address.

You can use the commands, **bgp bestpath as-path ignore**, **bgp bestpath compare-router-id** or **bgp bestpath med missing-as-worst** to customize the path selection process.

Example

This example shows how to configure to ignore the AS-PATH for the best path for autonomous system 65534.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp bestpath as-path ignore
```

10-7 bgp bestpath compare-confed-aspath

This command is used to configure a BGP routing process to compare the confederation AS path length of the routes received. To return the BGP routing process to the default operation, use the **no** form of this command.

bgp bestpath compare-confed-aspath

no bgp bestpath compare-confed-aspath

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If enabled, the BGP process will compare the confederation AS path length of the routes received. The shorter the confederation AS path length, the better the route is.

Example

This example shows how to enable BGP process to compare the AS path which contains some confederation as numbers.

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp bestpath compare-confed-aspath
```

10-8 bgp bestpath compare-routerid

This command is used to compare the router ID when comparing paths that have identical comparing factors. Use the **no** command to revert to the default behavior.

bgp bestpath compare-routerid

no bgp bestpath compare-routerid

Parameters

None.

Default

BGP selects the first route received as the best path when comparing paths that have identical comparing factors.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

By default, the BGP router does not consider router ID of the routes when comparing paths that have identical comparing factors. Use this command to include router ID in comparison of paths that have identical comparing factors.

Example

This example shows how to configure to compare router-id for identical eBGP paths for autonomous system 65534.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp bestpath compare-router-id
```

10-9 bgp bestpath med confed

This command is used to configure a BGP routing process to compare the Multi Exit Discriminator (MED) between paths learned from confederation peers. Use the **no** form of the command to disable MED comparison of paths received from confederation peers.

bgp bestpath med confed

no bgp bestpath med confed

Parameters

None.

Default

By default, MEDs are not compared between paths from confederation peers.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If enabled, the BGP process will compare the MED for the routes that are received from confederation peers. For routes that have an external AS in the path, the comparison does not occur.

Example

This example shows how to configure the BGP process 10000 to compare MED values for paths learned from confederation peers.

```
Switch# configure terminal
Switch(config)# router bgp 10000
Switch(config-router)# bgp bestpath med confed
```

10-10 bgp bestpath med missing-as-worst

This command is used to configure the router to assign a infinite value the route if missing MED. Use the **no** form of the command to restore the default setting.

bgp bestpath med missing-as-worst

no bgp bestpath med missing-as-worst

Parameters

None.

Default

MED 0 is assigned to the route if MED missed. MED 0 is treated as the best route.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

MED is an attribute that is exchanged between of eBGP neighbors. MED is an attribute specified by a local peer, and advertised to the remote peer to affect the best path selection result in the remote peer. The remote peer will not pass the MED value with routes for further path advertisement. The lower MED value is preferred than the larger MED value.

By default, MED 0 is assigned to a route if missing MED missing. Use the **bgp bestpath med missing-as-worst** command to configure the BGP router to assign a largest MED value to a route if missing MED.

Example

This example shows how to configure the BGP process 10000 to assign a largest MED value to a route if missing MED.

```
Switch# configure terminal
Switch(config)# router bgp 10000
Switch(config-router)# bgp bestpath med missing-as-worst
```

10-11 bgp client-to-client reflection

This command is used to enable route reflection from a BGP route reflector to clients. To disable client-to-client route reflection, use the **no** form of this command.

bgp client-to-client reflection

no bgp client-to-client reflection

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In a large scale BGP network, route reflection is a mechanism used to reduce the needs of fully mesh of iBGP sessions. With route reflection, an autonomous system can be partitioned into a number of clusters; each cluster is formed by the route reflector and its client. The connection between clusters is still fully meshed. However, in a cluster, the reflector needs to maintain connections with all clients, but the client does not need to maintain connections with other clients. The route reflector is responsible to reflect routes received from one client to other clients.

Use the **bgp client-to-client reflection** command on the route reflector to enable reflection of routes received from the clients to other clients. If the clients are already fully meshed, then use the **no bgp client-to-client reflection** command to disable client-to-client reflection because route reflection is not required.

Example

This example shows how to configure the local router is a route reflector with three neighbors as the clients. The client to client reflection is enabled to enable the route reflection.

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)#neighbor 10.20.0.1 route-reflector-client
Switch(config-router)#neighbor 10.20.0.2 route-reflector-client
Switch(config-router)#neighbor 10.20.0.3 route-reflector-client
Switch(config-router)# bgp client-to-client reflection
Switch(config-router)#
```

10-12 bgp cluster-id

This command is used to set the cluster ID in a route reflector cluster. To remove the cluster ID, use the **no** form of this command.

bgp cluster-id *CLUSTER-ID*

no bgp cluster-id

Parameters

CLUSTER-ID	Specifies to configure the cluster ID in the IPv4 address format

Default

The local router ID of the route reflector is used as the cluster ID when no ID is specified

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In a large scale BGP network, route reflection is a mechanism used to reduce the needs of fully mesh of iBGP sessions. With route reflection, an autonomous system can be partitioned into a number of clusters; each cluster is formed by the route reflector and its client. The connection between clusters is still fully meshed. However, in a cluster, the reflector needs to maintain connections with all clients, but the client does not need to maintain connections with other clients. The route reflector is responsible to reflect routes received from one client to other clients.

Each cluster is distinguished by a cluster ID. The cluster ID configured on the route reflector is the ID of the cluster. When cluster ID is not configured on the route reflector, the router ID of the reflector will be the cluster ID.

In a cluster, the user can define multiple route reflectors to provide redundancy and avoid the single point of failure, but these route reflectors must be configured with the same cluster ID. Use the **bgp cluster-id** command on the route reflector to configure the cluster ID on these route reflectors.

Example

This example shows how to configure the cluster has multiple route reflectors, and the local router as one of the route reflectors. It is configured with cluster ID 10.1.10.1.

```
Switch# configure terminal
Switch(config)# router bgp 100
Switch(config-router)# bgp cluster-id 10.1.10.1
```

10-13 bgp confederation identifier

This command is used to specify a BGP confederation identifier. Use the **no** form of this command to remove the confederation identifier.

bgp confederation identifier *AS-NUMBER*

no bgp confederation identifier

Parameters

AS-NUMBER	Specifies an Autonomous System number as a BGP confederation ID. The value is from 1 to 4294967295.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In a large scale BGP network, confederation is a mechanism used to reduce the needs of fully mesh of iBGP sessions. With confederation, an autonomous system can be partitioned into a number of a sub-AS. To the routers outside, the group of sub-AS appear as a single AS identified by the confederation ID.

Each sub-AS is fully meshed within the sub-AS itself and is connected to other sub-AS within the confederation. Route reflection can be used within the sub-AS to reduce the fully mesh. ,

Although peers in different sub-AS are connected by eBGP sessions, they exchange routing information as if they were iBGP peers. The next-hop, MED, and local preference information is preserved within the confederation.

Use the **bgp confederation identifier** command the specify the confederation ID, and use the **bgp confederation peer** command to configure the neighbor session for connection to another sub-AS within the same confederation.

Example

This example shows how to create a confederation in which the AS number is 20.

```
Switch# configure terminal
Switch(config)# router bgp 20
Switch(config-router)# bgp confederation identifier 20
```

10-14 bgp confederation peers

This command is used to add a BGP confederation peer. Use the **no** form of this command to delete a confederation identifier.

bgp confederation peers *AS-LIST*

no bgp confederation peers *AS-LIST*

Parameters

AS-LIST	Specifies one or multiple AS numbers for BGP peers separated by a comma. The specified AS is in the same confederation. The valid values are from 1 to 4294967295.

Default

By default, no confederation peer is configured.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In a large scale BGP network, confederation is a mechanism used to reduce the needs of fully mesh of iBGP sessions. With confederation, an autonomous system can be partitioned into a number of a sub-AS. To the routers outside, the group of sub-AS appear as a single AS identified by the confederation ID.

Each sub-AS is fully meshed within the sub-AS and is connected to another sub-AS within the confederation. Route reflection can be used within the sub-AS to reduce the fully mesh. Although peers in different sub-AS are connected by eBGP sessions, they exchange routing information as if they were iBGP peers. The next-hop, MED, and local preference information is preserved within the confederation.

Use the **bgp confederation identifier** command to specify the confederation ID and use the **bgp confederation peer** command to configure the neighbor session for connection to another sub-AS within the same confederation.

Example

This example shows how to configure the AS 21, 22, 23 as sub-ASs of a single confederation with confederation identifier 20.

```
Switch# configure terminal
Switch(config)# router bgp 20
Switch(config-router)# bgp confederation identifier 20
```

```
Switch(config-router)# bgp confederation peers 21,22,23
```

10-15 bgp dampening

This command is used to configure the route dampening function. Use the **no** form of the command to restore the default setting.

bgp dampening [*HALF-LIFE REUSE SUPPRESS MAX-SUPPRESS-TIME UN-REACHABILTY-HALF-TIME* **| route-map** *MAP-NAME***]**

no bgp dampening [route-map]

Parameters

HALF-LIFE	(Optional) Specifies the time (in minutes) after which the accumulated penalty of the route is decreased by half. The range of the half-life period is 1 to 45 minutes.
REUSE	(Optional) Specifies the penalty that is decreased and falls below the reuse threshold, the route will be re-entered the routing table as a normal route. The range of the reuse value is from 1 to 20000.
SUPPRESS	(Optional) Specifies the penalty that is increased and cross the suppress threshold, the route will become a dampening route and will not be advertised. The range is from 1 to 20000
MAX-SUPPRESS-TIME	(Optional) Specifies the maximum time (in minutes) that a route can be in the dampened state. The range is from 1 to 255. The default is 4 times the half-life.
UN-REACHABILITY-HALF-LIFE	Specifies the time (in minutes) after which the penalty of the unreachable routes will be down; by half.
route-map *MAP-NAME*	(Optional) Specifies the name of route map to control the routes for dampening.

Default

Half–life: 15 minutes.

Reuse: 750.

Suppress: 2000.

Max-suppress-time: 4 times half-life.

Un-reachability-half-life: 15 minutes.

Command Mode

Router Configuration Mode.

Address Family Mode (IPv4 unicast and VRF).

Command Default Level

Level: 12.

Usage Guideline

The purpose of this command is to eliminate the advertising of the unstable routes and thus to avoid unstable of the network caused by flapping routes.

When a prefix is removed or is added, BGP increases the penalty of the route by 1000. When the attribute of a received route has changes, BGP increases the penalty of the route by 500.

Supposed that half-life is configured as 15 min, reuse is 800, and suppress is 1500.

When a route flaps (from up to down), 1000 is added to the penalty of the route. Since the penalty is smaller than the suppress value, the route works normally. A withdraw message (an update message) is sent to the neighbors.

As the half-life timer expired, the penalty of the route becomes 500. If another flaps occur, the penalty of the route keep being increased. If it is larger than the suppress value, then the route will be dampened. BGP will not advertise message for the dampened route.

As the time passed, the penalty of the route decreased. If the penalty of the route falls below the reuse threshold, the route will be restored as a normal route and update message will be sent for the route.

If a route map is configured but the route map doesn't exist, it acts as all routes are enabled for dampening.

Example

This example shows how to configure the BGP process 10000. The BGP dampening values are set to 20 minutes for the half-life, 2500 for the reuse value, 8000 for the suppress value, and 80 minutes for the maximum suppress time.

```
Switch# configure terminal
Switch(config)# router bgp 10000
Switch(config-router)# bgp dampening 20 2500 8000 80 20
```

10-16 bgp default ipv4-unicast

This command is used to enable the exchange of IPv4 unicast routing information. Use the **no** command to disable the exchange of IPv4 unicast prefixes.

bgp default ipv4-unicast

no bgp default ipv4-unicast

Parameters

None.

Default

IPv4 unicast routing information exchange is enabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the router configuration mode to enable the exchange of IPv4 unicast routing information for all the subsequently created neighbor sessions. Use the **no bgp default ipv4-unicast** command to disable the automatic exchange of IPv4 unicast routing information.

Use the **neighbor activate** in address family configuration to activate the exchange of routing information of specific address family with a BGP neighbor.

Example

This example shows how to disable the exchange of IPv4 unicast address prefixes.

```
Switch# configure terminal
```

```
Switch(config)# router bgp 65534
Switch(config-router)# no bgp default ipv4-unicast
```

10-17 bgp default local-preference

This command is used to specify the default local preference value for the router. Use the **no** command to revert to the setting to default.

bgp default local-preference *NUMBER*

no bgp default local-preference

Parameters

NUMBER	Specifies the default local preference to apply to the routes received by this router. The range of the local reference is 0 to 4294967295.

Default

By default, this value is 100.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The local preference number is used to control the preferred exit point from the local AS to the same destination network. The local preference will be sent with the route advertised to the iBGP peers. If an external route is both reachable via the local router and an iBGP peer router, the local preference value determines the preferred exit point to reach the external route.

Use the **bgp default local-preference** command to specify the default local preference to be associated with the routes received by the router from external BGP peers.

Example

This example shows how to configure the default local preference of the router to be 200.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp default local-preference 200
```

10-18 bgp deterministic-med

This command is used to include the Multi Exit Discriminator (MED) value between all paths received from within the same autonomous system in the selection of the best route selection. Use the **no** command to prevent BGP from considering the MED attribute in comparing paths.

bgp deterministic-med

no bgp deterministic-med

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

All routers in a local AS must have the same setting of this command. When the **bgp always-compare-med** command is enabled, the Multi Exit Discriminator (MED) will be compared for paths from neighbors in different autonomous systems. When the **bgp deterministic-med** command is enabled, all paths destined for the same network that are received from neighbors in the same autonomous system , will be grouped together and sorted based on the ascending MED value. The sorting is performed right after the command is entered. The best path selection algorithm will then pick the best paths using the existing rules; the comparison is made on a per-neighbor autonomous system basis and then global basis.

If the **bgp deterministic-med** command is disabled, the paths will not be grouped and sorted.

Example

This example shows how to enable the compare MED value for autonomous system 65534.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp deterministic-med
```

10-19 bgp enforce-first-as

This command is used to enforce that the routes received from an eBGP peer must have the peer's AS number as the first AS in the AS path. Use the no command to disable this enforcement

bgp enforce-first-as

no bgp enforce-first-as

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enforce that the routes received from an eBGP peer must have the peer's AS number as the first AS in the AS path. This feature is used to avoid the local router from spoofing by a misconfigured peer.

Example

This example shows how to enable the security of the BGP network for autonomous system 65534. All incoming updates from eBGP peers are examined to ensure that the first AS number in the AS-path is the local AS number of the transmitting peer:

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp enforce-first-as
```

10-20 bgp fast-external-failover

This command is used to immediately reset an external BGP peering session if the link directly connected to the peer goes down. Use the **no** form of the command to disable BGP fast external failover.

bgp fast-external-failover

no bgp fast-external-failover

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to globally disable or enable fast external failover of BGP sessions for the directly connected external peers. When **fast-external-failover** is enabled, the session is immediately reset if the link goes down. When fast external failover is disabled, the session will not be reset until the default hold timer expires (3 keep alive times).

Example

This example shows how to configure the BGP fast external failover feature as disabled. If the link through which the session is carried flaps, the session will not be reset.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# no bgp fast-external-failover
```

10-21 bgp graceful-restart

This command is used to enable the BGP graceful restart capabilities for all BGP neighbors. Use the **no** form of this command to restore the router to its default state.

bgp graceful-restart [restart-time *RESTART-TIME* **| stalepath-time** *STALEPATH-TIME***]**

no bgp graceful-restart

Parameters

restart-time *RESTART-TIME*	Specifies the maximum time needed for neighbors to restart, in seconds. The value is from 1 to 3600.
stalepath-time *STALEPATH-TIME*	Specifies the maximum time to retain stale paths from restarting neighbors, in seconds. The value is from 1 to 3600.

Default

By default, the **restart-time** value is 120 seconds.

By default, the **stalepath-time** value is 360 seconds.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The **restart-time** parameter is used for setting the maximum time that a graceful restart neighbor waits to come back up after a restart. This value is applied to all neighbors unless you explicitly override it by configuring the corresponding value on the neighbor.

The **stalepath-time** parameter is used to set the maximum time to preserve stale paths from a gracefully restarted neighbor. All stale paths, unless reinstated by the neighbor after a re-establishment, will be deleted at the expiration of this timer.

When adjusting the timer values, the restart timer should not be set to a value greater than the hold time that is carried in the OPEN message.

Example

This example shows how to enable the BGP graceful restart capability for all BGP neighbors.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)# bgp graceful-restart
Switch(config-router)#
```

10-22 bgp router-id

This command is used to configure a router ID for the local Border Gateway Protocol (BGP) routing process. Use the **no** form of this command to remove the fixed router ID setting.

bgp router-id *IP-ADDRESS*

no bgp router-id

Parameters

IP-ADDRESS	Specifies the router ID in the IPv4 address format as the identifier of the local BGP router.

Default

A default router-ID will be assigned.

If loopback interfaces are not configured, the router ID is set to the highest IP address of interfaces.

If loopback interfaces are configured, the router ID is set to the highest IP address of loopback interfaces.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the router ID for the local BGP routing process. The router ID must be a uniquely assigned within the network.

Example

This example shows how to change the router ID to 192.168.1.1.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# bgp router-id 192.168.1.1
```

10-23 bgp scan-time

This command is used to configure the BGP scan timer value. The BGP router will periodically check whether the next hop is reachable from the BGP route. Use the **no** form of command to reset to default setting.

bgp scan-time *SCAN-INTERVAL*

no bgp scan-time

Parameters

SCAN-INTERVAL	Specifies the BGP scan timer value from 5 to 60 seconds.

Default

By default, this value is 60 seconds.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the router is enabled for scanning next hop of BGP routes, the router will periodically check whether there is a route to reach the next hop in the routing table.

Example

This example shows how to sets the scan-timer to 30 seconds.

```
Switch# configure terminal
```

```
Switch(config)# router bgp 100
Switch(config-router)# bgp scan-time 30
Switch(config-router)#
```

10-24 clear ip bgp

This command is used to reset Border Gateway Protocol (BGP) connections using hard or soft reconfiguration.

clear ip bgp [ipv4 unicast | vpnv4 {vrf *VRF-NAME* **| unicast}] {all |** *AS-NUMBER* **| peer-group** *PEER-GROUP-NAME* **|** *NEIGHBOR-ADDRESS***} [soft [in [prefix-filter] | out]]**

Parameters

ipv4	Specifies the IPv4 address family routing entry. It is the default address family.
unicast	Specifies the unicast address family routing entry. It is the default address family modifier.
vrf *VRF-NAME*	Specifies the VRF address family routing entry.
vpnv4	Specifies the IPv4 VPN address family routing entry.
all	Specifies to issue reset of all sessions in the specified address family.
AS-NUMBER	Specifies to issue reset of sessions with peers in the specified AS will be reset.
NEIGHBOR-ADDRESS	Specifies to issue reset of the specified neighbor session.
PEER_GROUP-NAME	Specifies to issue reset of the peer group sessions.
in	(Optional) Specifies to issue the inbound reconfiguration. If neither in nor out keyword is specified, both inbound and outbound sessions are reconfigured.
prefix-filter	(Optional) Specifies to clear the existing outbound route filter (ORF) prefix list to trigger a new route refresh to update the ORF prefix list from the peer router.
out	(Optional) Specifies to issue the outbound reconfiguration. If neither in nor out keyword is specified, both inbound and outbound sessions are reconfigured.
soft	(Optional) Specifies to issue a soft reset without tearing down the session.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to initiate a hard reset or a soft reset for a BGP session. If a soft reset is applied to outbound session, the router will re-transmit all the routes previously advertised to the specified neighbor

to refresh the routing entries in the neighbor peer. If a soft reset is applied to inbound session, the session will not be terminated but the local inbound routing table will be cleared and need to be rebuilt.

If soft reconfiguration inbound is enabled (use the command **neighbor soft-reconfiguration** in router configuration mode), then the routing table can be rebuilt based on the stored route updates information. If soft reconfiguration inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh. The user can use the **show ip bgp neighbors** command to check, if the peer router does not support the route refresh capability, then storing inbound route update information must be enabled to complete the inbound soft reconfiguration.

Whenever the following setting, which is applied to inbound session, is changed, the inbound routing table can be reconfigured by the inbound soft reset.

- BGP-related access lists
- BGP-related weights
- BGP-related prefix lists
- BGP-related route maps

When the inbound session is soft reset with the prefix filter option, if the capability ORF prefix list is enabled, in the receive mode, the local BGP will notify the remote neighbor to send the updated prefix filter.

Example

This example shows how to configure a soft reconfiguration that is initiated for the inbound sessions with the neighbor 10.100.0.1 and the outbound session is unaffected.

```
Switch# clear ip bgp 10.100.0.1 soft in
Switch#
```

This example show how to configure all member sessions in BGP peer group named INTERNAL to hard reset.

```
Switch# clear ip bgp peer-group INTERNAL
Switch#
```

This example shows how to configure a soft reconfiguration that is initiated for the inbound session with members of the peer group INTERNAL and the outbound session is unaffected.

```
Switch# clear ip bgp peer-group INTERNAL soft in
Switch#
```

10-25 clear ip bgp dampening

This command is used to clear BGP route dampening information.

clear ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME***] dampening [***IP-ADDRESS* **[***MASK-LENGTH***]]]**

Parameters

ipv4	Specifies the IPv4 address family routing entry. If not specified, the IPv4 unicast address family is the default address family.
unicast	Specifies the unicast address family routing entry.
vrf *VRF-NAME*	Specifies the VRF address family routing entry.
vpnv4	Specifies the IPv4 VPN address family routing entry.

IP-ADDRESS	(Optional) Specifies the routing prefix to clear the dampening information.
MASK-LENGTH	(Optional) Specifies the mask length for the IP address.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear dampening information in the routing table. If no arguments or keywords are specified, dampening information for the IPv4 unicast address family prefixes are cleared.

Example

This example shows how to clear route dampening information for the route prefix 192.168.10.0/24.

```
Switch# clear ip bgp dampening 192.168.10.0/24
Switch#
```

This example shows how to clear route dampening information for all IPv4 unicast address family prefixes.

```
Switch# clear ip bgp dampening
Switch#
```

10-26 clear ip bgp external

This command is used to reset external Border Gateway Protocol (eBGP) peering sessions using hard or soft reconfiguration.

clear ip bgp [ipv4 unicast] external [soft [in [prefix-filter] | out]]

Parameters

ipv4	Specifies to issue the reset of eBGP peering sessions for IPv4 address family.
unicast	Specifies to issue the reset of eBGP peering sessions for unicast address family sessions.
in	(Optional) Specifies to issue inbound reconfiguration. If neither in nor out keywords are specified, both inbound and outbound sessions are reset.
prefix-filter	(Optional) Specifies to clear the existing outbound route filter (ORF) prefix list to trigger a new route refresh to update the ORF prefix list from the peer router.
out	(Optional) Specifies to issue outbound reconfiguration. If neither the in nor out keywords are specified, both inbound and outbound sessions are reset.

soft	(Optional) Specifies to issue a soft reset without tearing down the session.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to initiate a hard reset or a soft reset for external BGP sessions.

Example

This example shows how to initiate a soft reconfiguration configured for all inbound eBGP peering sessions.

```
Switch# clear ip bgp external soft in
Switch#
```

10-27 clear ip bgp flap-statistics

This command is used to clear BGP route dampening flap statistics.

clear ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME***] flap-statistics [***IP-ADDRESS* **[***MASK-LENGTH***]]**

Parameters

ipv4	Specifies to clear an IPv4 address family routing entry.
unicast	Specifies to clear a unicast address family routing entry.
vrf *VRF-NAME*	Specifies the VRF address family routing entry.
vpnv4	Specifies the IPv4 VPN address family routing entry.
MASK-LENGTH	(Optional) Specifies the mask length for the IP address.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear the accumulated penalties for routes that have been received on a router which has BGP dampening enabled. If no arguments or keywords are specified, flap statistics of IPv4 unicast address family prefixes are cleared.

Example

This example shows how to clear flap statistics for all IPv4 unicast address prefixes.

```
Switch# clear ip bgp flap-statistics
Switch#
```

10-28 distance bgp

This command is used to configure the distance for BGP routes. Use the **no** form of the command to restore to the default setting.

distance bgp *EXTERNAL-DISTANCE INTERNAL-DISTANCE*

no distance bgp

Parameters

EXTERNAL-DISTANCE	Specifies the distance for routes learned from external peers. The valid range is 1 to 999.
INTERNAL-DISTANCE	Specifies the distance for routes learned from internal peers. The valid range is 1 to 999.

Default

External distance is 70.

Internal distance is 130.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

User can use the **distance bgp** command to set the administrative distance for routes learned from eBGP peers and iBGP peers. The **distance bgp** command acts as the distance command for other routing protocol, determines which routes will be installed in routing information base.

Numerically, an administrative distance is an integer from 1 to 999. In general, the higher the value is, the lower the rating of trustworthiness is.

Example

This example shows how to set the distance of external routes and internal routes in to 50, 100, respectively.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# distance bgp 50 100
```

10-29 ip as-path access-list

This command is used to define a rule entry for a BGP Autonomous System (AS) path access list. Use the **no** form of this command to remove the definition of an AS path access-list.

ip as-path access-list *ACCESS-LIST-NAME* **[{permit | deny}** *REGEXP***]**

no ip as-path access-list *ACCESS-LIST-NAME*

Parameters

ACCESS-LIST-NAME	Specifies the name of an AS path access list. The maximum length is 16 bytes
permit	Specifies that routes that match the rule entry are permitted.
deny	Specifies that routes that match the rule entry are denied.
REGEXP	Specifies a regular expression for the matching pattern.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to define an AS path access list entry. An AS path access list can contain multiple rule entries, either as a deny entry or a permit entry.

Use the **neighbor filter-list** command to apply an AS path access list to a neighbor session as an ingress filter or an egress filter. If an access list is applied, if the route matches an access list entry, then no further check will be done against other rules. If the match rule is a permit rule, then the route is permitted. If the matched rule is a deny rule, then the route is denied.

Use the **match as-path** command to match an access list in a route map entry definition. To match a route map entry, all match statements must be satisfied. To match an AS path access list, if an entry in the access list matches the route, then no further check will be done against the remaining entries in the access list. If the matched entry is a permit entry, then the AS path access list is matched. If the matched entry is a deny entry, then the AS path access list is not matched. If none of the rule entries in the AS path access list match the route, then the AS path access list is not matched.

Example

This example shows how to define an AS-path access-list called “mylist” to deny neighbors with the AS number 65535.

```
Switch# configure terminal
Switch(config)# ip as-path access-list mylist deny ^65535$
```

10-30 ip community-list

This command is used to add a community list entry. Use the **no** form of this command to delete the community list entry.

ip community-list standard *COMMUNITY-LIST-NAME* **[{deny | permit} [***COMMUNITY***] [***WELL-KNOWN-COMMUNITY***]]**

no ip community-list standard *COMMUNITY-LIST-NAME*

ip community-list expanded *COMMUNITY-LIST-NAME* **[{deny | permit}** *REGULAR-EXPRESSION***]**

no ip community-list expanded *COMMUNITY-LIST-NAME*

Parameters

standard	Specifies to configure a named standard community list.
expanded	Specifies to configure a named expanded community list.
COMMUNITY-LIST-NAME	Specifies the community list name. The maximum length is 16 bytes.
permit	Specifies that routes that match the rule entry are permitted.
deny	Specifies that routes that match the rule entry are denied.
COMMUNITY	(Optional) Specifies the community is a 32-bits integer. It can be a user-specified number represented by AA:NN, where AA (AS number) is the upper part of the word and NN (community number, user-specified) is the lower part of the word. Multiple numbers (separated by comma) can be specified.
WELL-KNOWN-COMMUNITY	(Optional) Specifies the well-known community by using the following keywords. Multiple numbers (separated by space) can be specified. **internet** - Specify routes free to be advertised to all peers. **local-as** - Specify not to send out of the local AS or sub autonomous system of a confederation. **no-advertise** - Specify not to advertise the route to other BGP peers. **no-export** - Specify not advertise to external peers.
REGULAR-EXPRESSION	Specifies to configure a regular expression that is used to specify a pattern to match against an input string. **Note:** Regular expressions can be used only with expanded community lists.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. A community attribute is represented by a 32 bits integer. If no community value is associated with a path, by default, the Internet community is associated with the path.

A community list can contain multiple rule entries, either as a deny entry or a permit entry. Use the command to define a community list rule entry.

A community list can be either a standard community list or an expanded community list. The rule entry defined in a standard community list contains a string formed by a number of communities, separated by space. The rule entry defined in an expanded community list contains a regular expression.

Use the **match community** command to match a community list in a route map entry definition. To match a route map entry, all match statements must be satisfied. To match a community list, if an entry in the community list matches the route, then no further check will be done against the remaining entries in the access list. If the matched entry is a permit entry, then the community list is matched. If the matched entry is a deny entry, then the community list is not matched. If none of the rule entries in the community list match the route, then the community list is not matched.

Example

This example shows how to configure a rule entry for a community list “mycommlist” that permits routes that from network 10 in autonomous system 50000.

```
Switch# configure terminal
Switch(config)# ip community-list standard mycommlist permit 50000:10
```

10-31 ip extcommunity-list

This command is used to add an extended community entry for VPN route filtering. Use the **no** form of this command to delete the extended community list entry.

ip extcommunity-list standard *EXTCOMMUNITY-LIST-NAME* **[{permit | deny}** *EXTCOMMUNITY***]**

no ip extcommunity-list standard *EXTCOMMUNITY-LIST-NAME*

ip extcommunity-list expanded *EXTCOMMUNITY-LIST-NAME* **[{permit | deny}** *REGEXP***]**

no ip extcommunity-list expanded *EXTCOMMUNITY-LIST-NAME*

Parameters

EXTCOMMUNITY-LIST-NAME	Specifies the extended community list name. The maximum length is 16 bytes. The syntax is general string that does not allow spaces.
permit	Specifies the extended community to accept.
deny	Specifies the extended community to reject.
EXTCOMMUNITY	Specifies the *EXT-COMMUNITY*. This consists of an RT value or an SOO value. It can accept 12 values for one entry. There are two different types for the RT value or SOO value: **IP address: number** - The IP address should be a global IP address that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be 1-65535. **AS Number: number** - The AS Number should be a public AS Number (Both 2-bytes AS number and 4-bytes AS number works) that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be 1 to 4294967295 for 2-bytes AS number and 1 to 65535 for 4-bytes AS number.
REGEXP	Specifies to configure a regular expression that is used to specify a pattern to match against an input string. Regular expressions can be used only with expanded community lists. The maximum length is 80 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The extended community attribute is used for implementing policy routing. It is an optional, transitive attribute and facilitates transfer of local policies through different autonomous systems. All the names of the standard **extcommunity** list and expended **extcommunity** list must not be the same.

This command can be applied multiple times. BGP extended community attributes exchanged between BGP peers are controlled by the neighbor send-community command.

If permit rules exist in an extended community list, routes with extended community that does not match any rule in the list will be denied. If there are no rules or only deny rules to be configured in the extended community list, all routes will be denied.

Example

This example shows how to define a standard extended community list named “myecom” with an entry.

```
Switch# configure terminal
Switch(config)# ip extcommunity-list standard myecom permit rt 1:1 soo 1.1.1.1:1
```

This example shows how to create an expanded extended community list named “myexpcom” with an entry.

```
Switch# configure terminal
Switch(config# ip extcommunity-list expanded myexpcom permit _20[0-9]
```

10-32 match as-path

This command is used to define a BGP AS-path access list match condition in a route map rule. To delete a match statement, use the **no** form of this command.

match as-path *ACCESS-LIST-NAME*

no match as-path

Parameters

ACCESS-LIST-NAME	Specifies an AS path access list name.

Default

No match statements in the route map.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A route map can contain multiple route map entries, which is either a permit entry or a deny entry. When a route is checked against a route map, the entry in the route map will be checked whether match the route based on its sequence number in the route map. If an entry is found matched, the action associated with the entry will be taken and no further check will be done against the remaining entry in the route map.

A route map entry can contain multiple match and set statements. To match a route against a route map entry, all of the match statements in the route map rule must be satisfied. When a route map entry is matched, all the set statements in the rule will be performed.

Use the **match as-path** command to match an access list in a route map entry. To match a route map entry, all match statements must be satisfied. To match an AS path access list, if an entry in the access

list matches the route, then no further check will be done against the remaining entries in the access list. If the matched entry is a permit entry, then the AS path access list is matched. If the matched entry is a deny entry, then the AS path access list is not matched. If none of the rule entries match the route, then the AS path access list is not matched.

Example

This example shows how to add a match statement to the policy routing entry named “myPolicy”.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
```

10-33 match community

This command is used to define a BGP community access list match condition in a route map rule. To delete the match statement, use the **no** form of this command.

match community *COMMUNITY-LIST-NAME* **[exact]**

no match community

Parameters

COMMUNITY-LIST-NAME	Specifies a BGP community access list.
exact	(Optional) Specifies that an exact match is required. All of the communities and only those communities specified must be present.

Default

No match statements in the route map.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A route map can contain multiple route map entries, which is either a permit entry or a deny entry. When a route is checked against a route map, the entry in the route map will be checked whether match the route based on its sequence number in the route map. If an entry is found matched, the action associated with the entry will be taken and no further check will be done against the remaining entry in the route map.

A route map entry can contain multiple match and set statements. To match a route map entry, all of the match statements in the route map rule must be satisfied. When a route map entry is matched, all the set statements in the rule will be performed.

Use the **match community** command to match a community list in a route map entry definition. To match a route against a route map entry, all match statements must be satisfied. To match a community list, if an entry in the community list matches the route, then no further check will be done against the remaining entries in the access list. If the matched entry is a permit entry, then the community list is matched. If the matched entry is a deny entry, then the community list is not matched. If none of the rule entries in the community list match the route, then the community list is not matched.

The **exact** keyword is used for matching a standard community list. When **exact** is specified, the communities of the route must be exactly the same as the communities specified in the community list entry.

When **exact** is not specified, to match a community list rule entry, the communities specified in the rule entry must be a subset of the communities specified in the community string of the route.

Example

This example shows how to configure the routes that match the community list “IT-COMMUNITY”, which permit 101:1, and the weight set to 100. Any route that has the community 101:1 alone (exact match) will have the weight set to 100.The route map is named “myPolicy”.

```
Switch# configure terminal
Switch(config)# ip community-list standard IT-COMMUNITY permit 101:1
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match community IT-COMMUNITY exact
Switch(config-route-map)# set weight 100
```

10-34 neighbor activate

This command is used to activate the exchange of routing information with a specified BGP neighbor. Use the **no** form of this command to deactivate the exchange with a specified BGP neighbor.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} activate**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} activate**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.

Default

The exchange of the IPv4 unicast address family is enabled by default.

The exchange for all other address families is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 unicast, VPNv4 and VRF).

Command Default Level

Level: 12.

Usage Guideline

If a BGP peer group is specified for the command, all the members of the peer group will inherit the setting configured with this command. The exchange of IPv4 unicast routing information with neighbors is enabled by default unless this default behavior is changed by the **no bgp default ipv4-unicast** command. Use the **no neighbor activate** command to disable the exchange of IPv4 unicast routing information with specific neighbors.

The exchange address family routing information other than IPv4 unicast with neighbors is disabled by default. Use the **neighbor activate** command to enable the exchange of a specific address family routing information with a specific neighbor.

Example

This example shows how to enable address exchange for the address family IPv4 multicast for neighbor 10.4.4.4.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router-af)# neighbor 10.4.4.4 activate
```

10-35 neighbor advertisement-interval

This command is used to configure the minimum interval between two BGP routing UPDATE messages. Use the **no** command to revert to the default setting.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} advertisement-interval** *SECONDS*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} advertisement-interval**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
SECONDS	Specifies the minimum interval, in seconds, between the sending of update messages. This value must be between 0 and 600.

Default

30 seconds for external peers.

5 seconds for internal peers.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (VRF).

Command Default Level

Level: 12.

Usage Guideline

If a BGP peer group is specified for the command, all the members of the peer group will inherit the setting configured with this command.

Example

This example shows how to set the minimum time between sending BGP routing updates to 15 seconds.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router=)# neighbor 10.4.4.4 advertisement-interval 15
```

10-36 neighbor allowas-in

This command is used to enable routers to allow their own AS appearing in the received BGP update packets. To disable a duplicate AS number, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} allowas-in [***NUMBER***]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} allowas-in**

Parameters

IP-ADDRESS	Specifies the IP address of a BGP peer.
PEER-GROUP-NAME	Specifies the name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
NUMBER	(Optional) Specifies the maximum number of local AS, allowed to appear in the AS-path attribute of update packets. The value is from 1 to 10. If no number is supplied, the default value of 3 times is used.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 Unicast, VPNv4 and VRF).

Command Default Level

Level: 12.

Usage Guideline

The BGP router will do AS path loop checks for the received BGP update packets. If the BGP router's own AS appears in the AS path list, it is identified as a loop and the packets will be discarded. If the **allowas-in** setting is enabled, the BGP router's own AS is allowed in the AS path list.

Example

This example shows how to set the number of times that the local router's own AS is allowed to appear in the update packets received from the neighbors 100.16.5.4 to 5.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)#neighbor 100.16.5.4 remote-as 65101
Switch(config-router)#neighbor 100.16.5.4 allowas-in 5
```

This example shows how to set the **allowas-in** to 3 without the *NUMBER* parameter.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)#neighbor 100.16.5.4 remote-as 65101
Switch(config-router)#neighbor 100.16.5.4 allowas-in
```

10-37 neighbor as-origination-interval

This command is used to configure the minimum interval between the sending of AS origination routing updates. Use the **no** command to revert to the default setting.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} as-origination-interval** *SECONDS*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} as-origination-interval**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
SECONDS	Specifies the minimum interval, in seconds, between the sending of AS origination routing update messages. This value must be between 1 and 600.

Default

By default, the interval value is 15 seconds.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (VRF).

Command Default Level

Level: 12.

Usage Guideline

AS origination routes can be generated by network, aggregate and redistribute commands. Use this command to configure the minimum interval value when sending these routes.

Example

This example shows how to set the AS origination interval of 15.1.1.52 to 100.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router=)# neighbor 15.1.1.52 as-origination-interval 100
```

10-38 neighbor as-override

This command is used to enable to override the AS number of a site with the provider's AS number on a PE router. Use the **no** form of the command to disable this function.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} as-override**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} as-override**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.

Default

By default, this option is disabled.

Command Mode

Address Family Configuration Mode (VRF).

Command Default Level

Level: 12.

Usage Guideline

The command is used to prevent routing loops between routers within a VPN.

In the VPN, the most typical application lies in that the two CE ends have the same AS number. Normally, these two CE routers can't receive the other from the other party, because the BGP protocol will not receive the route information with the same AS number in AS path attribute as the AS of BGP instance itself. After the above command is configured on the PE router, you can let the PE replace the AS number of the CE to AS number of PE self, so that the CE from the other end can receive the route information. Only set this function for the EBGP peer.

Example

This example shows how to enable the AS override flag of BGP peer 3.3.3.3 in VRF "vpn1".

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv4 vrf vpn1
Switch(config-router-af)# neighbor 3.3.3.3 remote-as 20
Switch(config-router-af)# neighbor 3.3.3.3 as-override
```

10-39 neighbor capability graceful-restart

This command is used to configure the router to advertise the graceful restart capability to the neighbors. Use the **no** form of this command to configure the switch so it does not advertise the graceful restart capability to its neighbor.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} capability graceful-restart**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} capability graceful-restart**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 Unicast and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

This configuration only indicates the BGP speaker that has the ability to preserve its forwarding state for some address families when BGP restarts. Use the **neighbor capability graceful-restart** command to advertise to the neighbor routers with the capability of graceful restart. The graceful restart capability is advertised only when the graceful restart capability has been enabled using the **bgp graceful-restart** command.

Example

This example shows how to enable to advertise the graceful restart capability for the IPv4 unicast address family to the neighbor 10.10.10.10.

```
Switch# configure terminal
```

```
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4 unicast
Switch(config-router)# neighbor 10.10.10.10 capability graceful-restart
Switch(config-router)#
```

10-40 neighbor capability orf prefix-list

This command is used to enable the advertisement of the ORF to a neighbor. Use the **no** form of the command to disable ORF.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} capability orf prefix-list {receive | send | both}**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} capability orf prefix-list {receive | send | both}**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of a Border Gateway Protocol (BGP) peer group.
receive	(Optional) Specifies to enable the receive mode of the ORF capability.
send	(Optional) Specifies to enable the send mode of the ORF capability.
both	(Optional) Specifies to enable both the send and receive mode of the ORF capability.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 unicast, VPNv4 and VRF).

Command Default Level

Level: 12.

Usage Guideline

The user can use the BGP ORF (Outbound Route Filtering) capability to reduce the number of prefixes exchanged with the peer. Typically, the command must be configured in pair on the local router and the remote router. The function can operate in one direction or in both directions. When it operates in one direction, the prefix list used as for the ingress filtering on one router will be sent to the peer router and act as the egress prefix list filtering applied to routes to be sent out from the peer router. The first router should be configured as send mode and the peer router should be configured as receive mode.

When the ingress prefix list on the first router is changed, to reflect the change to the peer router, the user should issue the **clear bgp in prefix-list** command on the peer router.

Example

In the following example, router A (10.20.30.5) is configured with ingress prefix list and is enabled for send mode and router B is enabled for receive mode. Router B (10.20.40.10) installs the egress prefix list from router by the **clear bgp in prefix-filter** command for the neighbor session.

Router A:

```
Switch# configure terminal
Switch(config)# router bgp 65100
```

```
Switch(config-router)# neighbor 10.20.40.10 remote-as 65200
Switch(config-router)# neighbor 10.20.40.10 prefix-list CUSTOMER in
Switch(config-router)# neighbor 10.20.40.10 capability orf prefix-list send
```

Router B:

```
Switch# configure terminal
Switch(config)# router bgp 65200
Switch(config-router)# neighbor 10.20.30.5 remote-as 65100
Switch(config-router)# neighbor 10.20.30.5 capability orf prefix-list receive
Switch(config-router)# exit
Switch(config)# exit
Switch# clear ip bgp 10.20.30.5 soft in prefix-filter
```

10-41 neighbor default-originate

This command is used to generate a default route to a neighbor. Use the **no** form of the command to disable generating the default route or disable the conditional injection.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} default-originate [route-map** *MAP-NAME***]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} default-originate**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
route-map *MAP-NAME*	(Optional) Specifies the name of a route map to achieve conditional injection of default route.

Default

No default route is sent to the neighbor.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 Unicast and VRF).

Command Default Level

Level: 12.

Usage Guideline

Use this command to inject the default route to a neighbor. The injection of a default route does not require the presence of 0.0.0.0 in the routing table. When the user specify the route map with the command, the default route will not be injected unless there is a route in the routing table that is permitted by the route map. If a route map is configured but the route map doesn't exist, it acts if the route map is not specified.

Example

This example shows how to configure the local router to inject the route 0.0.0.0 to the neighbor 172.16.2.3 unconditionally.

```
Switch# configure terminal
```

```
Switch(config)# router bgp 109
Switch(config-router)# network 172.16.0.0
Switch(config-router)# neighbor 172.16.2.3 remote-as 200
Switch(config-router)# neighbor 172.16.2.3 default-originate
```

10-42 neighbor description

This command is used to associate a description with a BGP neighbor. Use the **no** command to remove the description

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} description** *TEXT*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} description**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
TEXT	Specifies a descriptive string for the neighbor with a maximum of 80 characters. The syntax is a general string that allows spaces.

Default

None.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (VRF).

Command Default Level

Level: 12.

Usage Guideline

If you specify a BGP peer group for the command, all the members of the peer group will inherit the setting configured with this command.

Example

This example shows how to configure a description for the neighbor session with peer 172.16.10.10.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 172.16.10.10 description ABC in China
```

10-43 neighbor ebgp-multihop

This command is used to allow the router to establish a BGP session with an eBGP peer that is not directly connected to the local peer. Use the **no** command to revert to the default behavior.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} ebgp-multihop [***TTL***]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} ebgp-multihop**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
TTL	(Optional) Specifies the TTL value used for the BGP session.

Default

The eBGP peer must be directly connected to the router.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (VRF).

Command Default Level

Level: 12.

Usage Guideline

Use this command to allow the router to establish a BGP session with an eBGP peer that is not directly connected to the local peer. The user can specify the desired TTL value or not to specify to use the maximum TTL.

Example

This example shows how to allow the router to establish a BGP session with an eBGP peer 172.16.10.10 that is not directly connected to the local peer.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# network 10.108.0.0
Switch(config-router)# neighbor 172.16.1.1 ebgp-multihop
```

10-44 neighbor filter-list

This command is used to set up a BGP filter for the exchange of routing information with the specified neighbor. Use the **no** command to disable this function.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} filter-list** *AS-LIST-NAME* **{in | out}**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} filter-list** *AS-LIST-NAME* **{in | out}**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
AS-LIST-NAME	Specifies the name of an AS path access list. An AS path access list is defined by the **ip as-path access-list** command.
in	Specifies to apply the check for access lists in the ingress direction.
out	Specifies to apply the check for access lists in the egress direction.

Default

By default, no filter is used.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 unicast, VPNv4 and VRF).

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable AS path filtering based on a specified AS path access list. Use the **ip as-path access-list** command to create an AS path access list.

The **neighbor filter-list** command can be specified per address family. When specified, in the router configuration mode, the filter list is applied to the IPv4 unicast address family only.

The user can specify one filter list per address family for outbound routes to a BGP neighbor and one filter list for inbound routes from a BGP neighbor.

Example

This example shows how to define an AS path access list and applies it to filter the routes to be advertised to the neighbor 172.16.1.1.

```
Switch# configure terminal
Switch(config)# ip as-path access-list myacl deny _123_
Switch(config)# ip as-path access-list myacl deny ^123$
Switch(config)# ip as-path access-list myacl permit .*
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 192.168.6.6 remote-as 123
Switch(config-router)# neighbor 172.16.1.1 remote-as 47
Switch(config-router)# neighbor 172.16.1.1 filter-list myacl out
```

10-45 neighbor maximum-prefix

This command is used to specify the maximum number of prefixes that can be accepted from a neighbor. To disable the limitation, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} maximum-prefix** *MAXIMUM* **[***THRESHOLD***] [warning-only]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} maximum-prefix**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor.
PEER-GROUP-NAME	Specifies the name of a Border Gateway Protocol (BGP) peer group.
MAXIMUM	Specifies the maximum number of prefixes acceptable from the specified neighbor. This value must be between 1 and 12000.
THRESHOLD	(Optional) Specifies the percentage of the maximum prefix limit to generate a warning message. The range is from 1 to 100. The default value is 75.
warning-only	(Optional) Specifies only to generate a system log message when the threshold is exceeded. If not specified, the peering session will be

	terminated when the threshold is exceeded.

Default

By default, the maximum number of prefix value is 16000.

The threshold value is 75 percent.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 unicast, VPNv4 and VRF).

Command Default Level

Level: 12.

Usage Guideline

The user can use the **maximum-prefix** command to configure a maximum number to restrict the number of routing prefixes that can be accepted from the specified peer. To use the command, the user should determine the maximum number of prefixes based on the amount of available system resources.

When the maximum number is defined for a session, the system will monitor whether the current prefix number exceed the threshold. When the threshold is exceeded, if the option **warning-only** is not specified, the session will be terminated and a system message will be generated to notify the user of the event. If the **warning-only** option is specified, a system message will be generated to notify the user of the event. If a session is terminated due to exceeding of the maximum prefixes, the session will not be rebuilt unless the **clear ip bgp** command is issued to do a hard reset on the session.

Example

This example shows how to set the maximum prefixes that will be accepted from the neighbor, 192.168.1.1 to 1000.

```
Switch# configure terminal
Switch(config)# router bgp 40000
Router(config-router)# network 192.168.0.0
Router(config-router)# neighbor 192.168.1.1 maximum-prefix 1000
```

10-46 neighbor next-hop-self

This command is used to configure the router as the next hop for a BGP-speaking neighbor or peer-group. To disable this feature, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} next-hop-self**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} next-hop-self**

Parameters

IP-ADDRESS	Specifies the IP address of the BGP-speaking neighbor.
PEER-GROUP-NAME	Specifies the name of a BGP peer group.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration Mode (IPv4 unicast, VPNv4 and VRF).

Command Default Level

Level: 12.

Usage Guideline

To advertise a route to an eBGP peer, the BGP router will use the original next hop of the advertised route as the next hop if the original next hop is in the same subnet as the router's advertising interface. This will create problem if the attaching interface is an unmeshed network where BGP neighbors may not have direct access to all other neighbors on the same IP subnet. Use the **neighbor next-hop-self** command to use the router's self IP address as the next-hop of the routes for this case.

Example

This example shows how to force all updates destined for 10.108.1.1 to advertise this router as the next hop.

```
Switch# configure terminal
Switch(config)# router bgp 40000
Router(config-router)# neighbor 10.108.1.1 next-hop-self
Router(config-router)#
```

10-47 neighbor password

This command is used to enable Message Digest 5 (MD5) authentication and set the password on a TCP connection between two BGP peers. Use the **no** command to disable this function.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} password** *PASSWORD*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} password**

Parameters

IP-ADDRESS	Specifies the IP address of the BGP peer.
PEER-GROUP-NAME	Specifies the name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.
PASSWORD	Specifies the clear text password. The password is used when the TCP connection between BGP neighbors is established. This password can be up to 25 characters long.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the password for a BGP neighbor or BGP peer group. The password setting will cause TCP connections between the peers to restart with MD5 authentication. The same password need be configured between peers; otherwise the TCP connection will fail.

When using this command, the BGP connection will be torn down. After a while, the connection will be rebuilt if both the BGP speakers are configured with the same password.

Example

This example shows how to set the password of the BGP neighbor 10.2.2.2 to “abc”.

```
Switch# configure terminal
Switch(config)# router bgp 40000
Switch(config-router)# neighbor 10.2.2.2 remote-as 30000
Switch(config-router)# neighbor 10.2.2.2 password abc
Switch(config-router)#
```

10-48 neighbor peer-group (create group)

This command is used to create a peer group. Use the **no** command to remove a peer group.

neighbor *PEER-GROUP-NAME* **peer-group**

no neighbor *PEER-GROUP-NAME* **peer-group**

Parameters

PEER-GROUP-NAME	Specifies the name of the BGP peer group

Default

By default, no peer group is created.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

In many cases, multiple remote neighbors may share the same attribute settings. To simplify the task of configuration, it is useful to group a number of neighbors into a peer group and configure the command on the peer group.

Example

This example shows how to create a peer group, named NEW-GROUP.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor NEW-GROUP peer-group
```

10-49 neighbor peer-group (add group member)

This command is used to add a neighbor in a peer group. Use the **no** command to remove a neighbor from a peer group.

neighbor *IP-ADDRESS* **peer-group** *PEER-GROUP-NAME*

no neighbor *IP-ADDRESS* **peer-group** *PEER-GROUP-NAME*

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.

Default

None.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast, VPNv4 and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

The neighbor at the specified IPv4/IPv6 address inherits all the configured options of the peer group.

In many cases, multiple remote neighbors may share the same attribute settings. To simplify the task of configuration, it is useful to group a number of neighbors into peer group and configure the command on the peer group.

If a group has the **remote-as** setting, if a group member joined that peer group, the group member will have that remote AS or change to that remote AS if the member neighbor already has connection. After a neighbor joined that peer group, the group member's remote AS cannot be changed.

If a peer group has no remote AS setting, then a member that has no remote AS configured is not allowed to join this peer group. The group member can have its own configured remote AS. If remote AS is set for the peer group later, all group member's remote AS will be changed to the same remote AS.

After a neighbor joined a peer group, the following command will be prohibited to be configured on the individual neighbor: **neighbor timers**, **neighbor filter-list**, **neighbor route-map**.

If the user configures a neighbor command on a peer group, all the members of the peer group will inherit the characteristic configured with this command. If later the user configures the command on member of the peer group (if the command is allowed), the command setting configured for the group member takes effect.

If the user configures the command setting on member of the group, and later configures the command setting on the peer group again, the setting for the group member will disappear and thus the setting for the peer group takes effect.

Example

This example shows how to add a group member 10.1.1.254 to the peer group, named NEW-GROUP.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor NEW-GROUP peer-group
Switch(config-router)# neighbor 10.1.1.254 remote-as 100
Switch(config-router)# neighbor 10.1.1.254 peer-group NEW-GROUP
```

10-50 neighbor prefix-list

This command is used to prevent the distribution of the Border Gateway Protocol (BGP) neighbor information as specified in a prefix list, a Connectionless Network Service (CLNS) filter expression, or a CLNS filter set. To remove a filter list, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} prefix-list** *PREFIX-LIST-NAME* **{in | out}**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} prefix-list** *PREFIX-LIST-NAME* **{in | out}**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
PREFIX-LIST-NAME	Specifies the name of a prefix list.
in	Specifies the filter list applied to paths advertised from the neighbor.
out	Specifies the filter list applied to paths to be advertised to the neighbor.

Default

All external and advertised address prefixes are distributed to BGP neighbor.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast, VPNv4 and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

The **neighbor prefix-list** command can be specified per address family. When specified in the router configuration mode, the prefix-list is applied to the IPv4 unicast address family only.

The user can specify one prefix-list per address family for outbound routes to a BGP neighbor and one prefix-list for inbound routes from a BGP neighbor.

Example

This example shows how to apply the prefix list named “MyACL” to incoming route advertisements from the neighbor 10.1.1.240.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# network 172.10.1.2
Switch(config-router)# neighbor 10.1.1.240 prefix-list MyACL in
```

10-51 neighbor remote-as

This command is used to add an entry to the Border Gateway Protocol (BGP) neighbor table. Use the **no** form of this command to remove an entry from the table.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} remote-as** *AS-NUMBER*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} remote-as**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor.
PEER-GROUP-NAME	Specifies the name of a BGP peer group.
AS-NUMBER	Specifies the number of the autonomous system to which the neighbor belongs. The range is from 1 to 4294967295.

Default

There are no BGP neighbor peers.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used to create a BGP neighbor by specifying the IPv4 address of the neighbor and the AS number where the neighbor is located. A local router can establish peer relation with multiple BGP routers. The BGP peer can be an external peer or an internal peer. If the AS number specified for the neighbor is the same as the local AS number, then the neighbor is an internal neighbor. Otherwise, the neighbor is an external neighbor.

The remote AS command is fundamental to create a neighbor. A neighbor must have a remote AS specified in order to configure other neighbor commands. The remote AS of a neighbor is specified by either the remote as setting for the neighbor or by the remote as setting for the peer group that the neighbor joined.

By default, neighbors that are defined using the **neighbor remote-as** command in router configuration mode exchange only unicast address prefixes. To exchange other address prefix types, such as VPNv4 neighbors must also be activated using the **neighbor activate** command in address family configuration mode.

Example

This example shows how to specify that the router at the address 10.108.2.1 is a neighbor in the autonomous system number 110.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# network 10.108.0.0
Switch(config-router)# neighbor 10.108.2.1 remote-as 110
```

10-52 neighbor remove-private-as

This command is used to remove private autonomous system numbers in the AS path list of the outbound update routes. To disable this function, use the **no** form of this command.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} remove-private-as**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} remove-private-as**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor.
PEER-GROUP-NAME	Specifies the name of a BGP peer group.

Default

This command is disabled by default.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can only be configured for external BGP (eBGP) neighbor sessions. The private autonomous system values are from 64512 to 65535. If the setting is enabled, the BGP router will check the AS path list for routes outbound to the specific neighbor and remove the private AS number if it is present in the AS path list.

Example

This example shows how to remove the private autonomous system number for prefix sent to 10.108.1.1 and removes the private autonomous system number for the IPv4 unicast address family prefixes sent to 172.16.2.33.

```
Switch# configure terminal
Switch(config)# router bgp 100
switch(config-router)# neighbor 10.108.1.1 description peer with private-as
switch(config-router)# neighbor 10.108.1.1 remote-as 65001
switch(config-router)# neighbor 10.108.1.1 remove-private-as
switch(config-router)# neighbor 172.16.2.33 remote-as 2051
switch(config-router)# address-family ipv4 unicast
switch(config-router-af)# neighbor 172.16.2.33 remove-private-as
switch(config-router-af)#
```

10-53 neighbor route-map

This command is used to apply a route map to incoming or outgoing routes. Use the **no** command to remove the route map.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} route-map** *MAP-NAME* **{in | out}**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} route-map** *MAP-NAME* **{in | out}**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
MAP-NAME	Specifies the name of a route map.
in	Specifies that the route map is applied to paths advertised from the neighbor.

out	Specifies that the route map is applied to the paths advertised to the neighbor.

Default

None.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast, VPNv4 and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

The **neighbor route-map** command can be specified per address family. When specified in the router configuration mode, the route map is applied to the IPv4 unicast address family only.

The user can specify one route map per address family for outbound routes to a BGP neighbor and one route map for inbound routes from a BGP neighbor.

Example

This example shows how to apply a route map named internal-map to a BGP outgoing route from 172.16.70.24.

```
Switch# configure terminal
Switch(config)# router bgp 5
Switch(config)# neighbor 172.16.70.24 route-map internal-map out
Switch(config)# route-map internal-map
Switch(config-route-map)# match as-path 1
Switch(config-route-map)# set local-preference 100
Switch(config-route-map)#
```

10-54 neighbor route-reflector-client

This command is used to configure the router as a BGP route reflector and assign the specified neighbor as its client. Use the **no** form of this command to remove the neighbor from the client list.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} route-reflector-client**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} route-reflector-client**

Parameters

IP-ADDRESS	Specifies the IP address of the neighboring router.
PEER-GROUP-NAME	Specifies the peer group to act as the route reflector client.

Default

No route reflector client is configured.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast and VPNv4) Mode.

Command Default Level

Level: 12.

Usage Guideline

If a BGP peer group is specified for the command, all the members of the peer group will inherit the setting configured with this command.

In a large scale BGP network, route reflection is a mechanism used to reduce the needs of full mesh of iBGP sessions. With route reflection, an autonomous system can be partitioned into a number of clusters. Each cluster is formed by the route reflector and its client. The connection between clusters is still fully meshed. However, in a cluster, the reflector needs to maintain connections with all clients, but the client does not need to maintain connections with other clients. The route reflector is responsible to reflect routes received from one client to other clients.

Use the **neighbor route-reflector-client** command on the route reflector to configure the route reflection client. When a router is configured with the route reflection clients, the router becomes the route reflector. Use the **bgp cluster-id** command to configure the cluster ID when a cluster has more than on route reflector. Use the **no bgp client-to-client reflection** command to disable the route reflection when the connections between clients are already fully meshed.

Example

This example shows how to add a neighbor as the route reflector client.

```
Switch# configure terminal
Switch(config)# router bgp 50
Switch(config)# address-family ipv4
Switch(config-router-af)# neighbor 10.20.10.2 remote-as 50
Switch(config-router-af)# neighbor 10.20.10.2 route-reflector-client
```

10-55 neighbor send-community

This command is used to specify to send the specified type of community attributes to a BGP neighbor. Use the **no** form of this command to disable sending of the specified type of community attributes.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} send-community [both | standard | extended]**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} send-community [both | standard | extended]**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
both	Specifies to send or not to send both standard and extended community.
standard	Specifies to send or not to send the standard community.
extended	Specifies to send or not to send the extended community.

Default

The community attributes will not be sent.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast, VPNv4 and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

The **neighbor send-community** command can be specified per address family. When specified in the router configuration mode, the route map is applied to the IPv4 unicast address family only. If no community value is associated with a path, by default, the Internet community is associated with the path. The parameters, both and extended, are only supported in the VPNv4 address family.

Example

This example shows how to configure VPNv4 address family prefixes to the send-community with both standard and extended.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# address-family vpnv4
Switch(config-router-af)# neighbor 10.4.4.4 send-community both
```

10-56 neighbor shutdown

This command is used to disable a neighbor or a peer group. Use the **no** form of this command to re-enable a neighbor or a peer group.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} shutdown**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} shutdown**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.

Default

None.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

The user can use this command to terminate the active session for the specified neighbor or to terminate the active session for all members of a peer group. When a session is shutdown, all the associated routing information will be removed.

Example

This example shows how to disable any active session for the neighbor 172.16.10.10.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 172.16.10.10 shutdown
```

10-57 neighbor soft-reconfiguration

This command is used to enable the storing of the route information update from the neighbor peer. Use the **no** form of the command to disable the storing of the route update information.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} soft-reconfiguration inbound**

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} soft-reconfiguration inbound**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

If a soft reset is applied to inbound sessions. The session will not be terminated, but the local inbound routing table will be cleared and it needs to be rebuilt.

If soft reconfiguration inbound is disabled, then the local router will send the route refresh request to the neighbor to ask for the route refresh. If soft reconfiguration inbound is enabled, then the routing table can be rebuilt based on the stored route updates information. Enabling of the soft reconfiguration feature will consume extra system resource to store the route.

The user can use the **show ip bgp neighbors** command to see whether the neighbor supports the route refresh capability. If the neighbor supports the refresh capability, the inbound routing table can be rebuilt by refresh of the routing information.

Example

This example shows how to enable the storing of route update information for the neighbor peer session 10.100.0.1 since the peer does not support route refresh function.

```
Switch(config-router)# neighbor 10.100.0.1 soft-reconfiguration inbound
Switch(config-router)#
```

10-58 neighbor soo

This command is used to configure the Site-of-Origin (SoO) value of a peer or a peer group. Use the **no** form of this command to remove the SoO value configured.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} soo** *SOO-VALUE*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} soo**

Parameters

IP-ADDRESS	Specifies the address of the peer.
PEER-GROUP-NAME	Specifies the name of the peer group,
SOO-VALUE	Specifies that the Site-of-Origin attribute will be encoded as a Route Origin Extended Community. There are two different types of attributes: **IP address:number:** The IP address should be a global IP address that is assigned to the user and the number is assigned from a numbering space that is administered by the user. This number must be between 1 and 65535. **AS Number:number:** The AS Number should be a public AS Number (Both 2-bytes AS number and 4-bytes AS number works) that is assigned to the user and the number is assigned from a numbering space that is administered by the user. The number can be between 1 and 4294967295 for a 2-bytes AS number and 1 and 65535 for a 4-bytes AS number.

Default

No SoO value is set.

Command Mode

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to set the SoO value for a BGP neighbor or a peer group. The SoO extended community is BGP extended communities attribute that is used to identify routes that have originated from a site so that the re-advertisement of that prefix back to the source site can be prevented. The SoO extended community uniquely identifies the site from which a router has learned a route. BGP can use the SoO value associated with a route to prevent routing loops.

Example

This example shows how to set the SoO value of BGP peer 3.3.3.3 in VRF vpn1.

```
Switch# configure terminal
Switch(config)# router bgp 10
Switch(config-router)# address-family ipv4 vrf vpn1
Switch(config-router-af)# neighbor 3.3.3.3 remote-as 20
Switch(config-router-af)# neighbor 3.3.3.3 soo 10:100
Switch(config-router-af)# exit
```

10-59 neighbor tcp-reconnect

This command is used to set the minimum interval that BGP tries another TCP connection to the peer after a TCP connection fail happens. Use the **no** command to revert to the default setting.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} tcp-reconnect** *SECONDS*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} tcp-reconnect**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor.
PEER-GROUP-NAME	Specifies the name of a BGP peer group.
SECONDS	Specifies the minimum interval value that BGP tries another TCP connection. This value must be between 1 and 65535 seconds.

Default

By default, this value is 120 seconds.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

If the TCP connection to the neighbor fails, BGP will try another TCP connection to the neighbor after the TCP reconnect time. This command is used to configure the time interval of the TCP reconnect time.

Example

This example shows how to set the connect time of 14.1.1.52 to 90 seconds.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 14.1.1.52 tcp-reconnect 90
Switch(config-router)#
```

10-60 neighbor timers

This command is used to configure the BGP timers for a specific BGP peer or a peer group. Use the **no** form of this command to remove the timers setting.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} timers** *KEEP-ALIVE HOLD-TIME*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} timers**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
KEEP-ALIVE	Specifies the time interval for sending keep-alive messages to the specified peer. The range is from 0 to 65535.
HOLD-TIME	Specifies the time interval to declare a pear dead if the keep-alive messages is timeout. The range is from 0 to 65535.

Default

KEEPALIVE: 60 seconds.

HOLDTIME: 180 seconds.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

The timers configured for a specific neighbor or peer group override the timers configured for all BGP neighbors using the **timers bgp** command. If the minimum acceptable hold time is configured, the BGP session will only be established when the remote peer is equal to or greater than the minimum hold time.

Example

This example shows how to configure the *KEEP-ALIVE* timer to 120 seconds and *HOLD-TIME* timer to 360 seconds for the neighbor 172.16.10.10.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 172.16.10.10 timers 120 360
```

10-61 neighbor unsuppress-map

This command is used to selectively advertise routes that are previously suppressed by the aggregate-address command. Use the **no** form of this command to remove the unsuppressed route map.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} unsuppress-map** *MAP-NAME*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} unsuppress-map**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor router.
PEER-GROUP-NAME	Specifies the neighbor peer group.
MAP-NAME	Specifies the route map to selectively unsuppress the routes suppressed by the **aggregate-address** command.

Default

No routes are unsuppressed.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast, VPNv4 and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

When a route map is applied by the **neighbor unsuppress-map** command, the suppressed route that matches the permit rule will be unsuppressed. It provides manipulation of routes per neighbor.

Example

This example shows how to show the routes specified by a route map named internal-map being unsuppressed for neighbor 172.16.10.10.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# address-family ipv4
Switch(config-router-af)# neighbor 172.16.10.10 unsuppress-map internal-map
```

10-62 neighbor update-source

This command is used to allow a BGP session to use any operational interface's IP address as the source address to initiate the TCP connections. Use the **no** form of this command to restore the interface assignment to the closest interface.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} update-source** *INTERFACE-TYPE INTERFACE-NUMBER*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} update-source**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
INTERFACE-TYPE	Specifies the type of the interface. The supporting types are VLAN interface and loopback interface.
INTERFACE-NUMBER	Specifies the number of the interface. The interface number's range is from 1 to 8 for the loopback interface and from 1 to 4094 for the VLAN interface.

Default

The best local address is used.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify any operating interface as the source interface for the BGP session. By default, the BGP router will choose an interface closest to the remote peer. The loopback interface is most commonly used with this command. The use of the loopback interface eliminates the dependency on the availability of a particular interface for making TCP connections.

Example

This example shows how to configure the internal BGP sessions to use VLAN 1 for the neighbor 172.16.10.10.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 172.16.10.10 update-source vlan 1
```

10-63 neighbor weight

This command is used to specify the weight assigned to the routes that are received from a specific neighbor. Use the **no** form of this command to revert to the default setting.

neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} weight** *NUMBER*

no neighbor {*IP-ADDRESS* **|** *PEER-GROUP-NAME***} weight**

Parameters

IP-ADDRESS	Specifies the IP address of the neighbor peer.
PEER-GROUP-NAME	Specifies the name of the BGP peer group.
NUMBER	Specifies the weight number. The range is from 0 to 65535.

Default

The default weight assigned to routes received from a BGP peer is 0.

The default weight assigned to routes sourced by the local route is 32768.

Command Mode

Router Configuration Mode.

Address Family Configuration (VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

BPG weight is an attribute that is assigned by the local router to affect the best path selection on the local router. Use this command to specify the weight to be associated the routes learned from the specified neighbor. The route with highest weight will be chosen as the preferred route. If route map set weight to a route, then the route map specified weight will override the weight specified by the neighbor weight command. Weight is an attribute which is specified in ingress direction, and is not an attribute to be advertised with route, it is used to specify preference to routes received from a neighbor over another neighbor.

Example

This example shows how to set the weight of the neighbor 10.4.4.4 to 10000.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# neighbor 10.4.4.4 weight 10000
```

10-64 network (BGP)

This command is used to configure the networks to be advertised by the Border Gateway Protocol (BGP) process. To remove an entry from the routing table, use the **no** form of this command.

network *NETWORK-NUMBERISUBNET-LENGTH* **[route-map** *MAP-NAME***]**

no network *NETWORK-NUMBERISUBNET-LENGTH* **[route-map]**

Parameters

NETWORK-NUMBER	Specifies the network number that BGP will advertise.
SUBNET-LENGTH	Specifies the length of the network or sub-network.
route-map *MAP-NAME*	(Optional) Specifies the identifier of a route map. The configured network must be permitted by the specified route map to be advertised.

Default

None.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used to specify a network in the local AS. The network is added in the routing table, and will be advertised to the external neighbor peer. BGP networks can be learned from connected routes, from dynamic routing, and from static route sources.

Use this command to specify a network as local to this autonomous system and adds it to the BGP routing table. For exterior protocols the network command controls which networks are advertised. Interior protocols use the network command to determine where to send updates.

Example

This example shows how to set up network 10.108.0.0 to be included in the BGP updates for AS number is 65100.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# network 10.108.0.0/16
```

10-65 redistribute

This command is used to redistribute routes from one routing domain into BGP. Use the **no** command to disable route redistribution.

redistribute {connected | static | rip | ospf {all | internal | external | type-1 | type-2 | inter+e1 | inter+e2}} [metric *METRIC-VALUE* **| route-map** *MAP-NAME***]**

no redistribute {local | static | rip | ospf} [metric | route-map]

Parameters

connected	Specifies to redistribute connected routes to BGP.
static	Specifies to redistribute static routes to BGP.
rip	Specifies to redistribute RIP routes to BGP.
ospf	Specifies to redistribute OSPF routes to BGP. **all** - Specifies to redistribute both OSPF AS-internal and OSPF AS-

	external routes to BGP. **internal** - Specifies to redistribute only the OSPF AS-internal routes. **external** - Specifies to redistribute only the OSPF AS-external routes, including type-1 and type-2 routes. **type-1** - Specifies to redistribute only the OSPF AS-external type-1 routes. **type-2** - Specifies to redistribute only the OSPF AS-external type-2 routes. **inter+e1** - Specifies to redistribute only the OSPF AS-external type-1 and OSPF AS-internal routes. **inter+e2** - Specifies to redistribute only the OSPF AS-external type-2 and OSPF AS-internal routes.
metric *METRIC-VALUE*	(Optional) Specifies the BGP metric value for the redistributed routes. Enter the metric value used here. This value must be between 0 and 4294967295.
route-map *MAP-NAME*	(Optional) Specifies the identifier of a route map used to filter the networks to be redistributed. If not specified, all networks are redistributed.

Default

By default, route redistribution is disabled.

Command Mode

Router Configuration Mode.

Address Family Configuration (IPv4 unicast and VRF) Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used to redistribute the prefix from different sources to the BGP protocol. If the specified route map does not exist, the command acts as if the route map is not specified.

Example

This example shows how to redistribute the OSPF routes into the BGP process.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# redistribute ospf all
Switch(config-router)#
```

10-66 router bgp

This command is used to configure and enable the BGP routing process and enter the BGP router configuration mode. Use the **no** command to remove a BGP routing process.

router bgp *AS-NUMBER*

no router bgp *AS-NUMBER*

Parameters

AS-NUMBER	Specifies the number of an autonomous system that identifies the router to other BGP routers. This value must be between 1 and 4294967295.

Default

No BGP routing process is enabled by default.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A BGP router can only have one BGP routing process. Each BGP routing process needs to be associated with an autonomous system number.

The AS Number is defined as a 2 byte number in RFC1771 and RFC4271. In RFC 4893, the autonomous number is expanded to 4 bytes in order to support larger number of autonomous number.

Each public autonomous system that directly connects to the Internet needs to have a public assigned unique number (a number from 1 to 64511). Private autonomous system numbers are in the range from 64512 to 65534 (65535 is reserved for special use).

Private autonomous system numbers can be used for internal routing domains but must be translated for traffic that is routed out to the Internet. BGP routers should not be configured to advertise private autonomous system numbers to external networks.

Use this command to enter BGP router configuration mode for the specified routing process.

Example

This example shows how to configure a BGP process for autonomous system 65534.

```
Switch# configure terminal
Switch(config)# router bgp 65534
Switch(config-router)#
```

10-67 set as-path

This command is used to specify a statement in a route map to modify an autonomous system path for BGP routes. To delete an entry, use the **no** form of this command.

set as-path prepend *AS-PATH-STRING*

no set as-path prepend

Parameters

AS-PATH-STRING	Specifies an AS path string which will be prepended to the path list of the matched routes. An AS number or a list of AS numbers separated by comma can be specified.

Default

There is no set AS-path statement.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The AS path length is an important factor, that affects the best path selection. When the as-path is not modified by the route map the local AS is prepended to the existing AS path list. By using **set as-path prepend** to “prepend” an additional autonomous system path string to the AS path of the BGP routes (This is usually done by prepending the local autonomous system number multiple times to increase the autonomous system path length), a BGP router can influence the best path selection by the peer.

You can verify your settings by entering the **show route-map** command.

Example

This example shows how to set the as-path list 1, 10, 100, 200 with route map entry myPolicy.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)#set as-path prepend 1,10,100,200
```

10-68 set community

This command is used to set the BGP communities attribute. To delete an entry, use the **no** form of this command.

set community {*COMMUNITY-NUMBER* **[***WELL-KNOWN-COMMUNITY***] [additive]}**

no set community

Parameters

COMMUNITY-NUMBER	Specifies the community number is a four bytes integer. It is presented in a “AA:NN” format and the AA and the NN both are numbers from 1 to 65535. Multiple community numbers can be specified.
WELL-KNOWN-COMMUNITY	(Optional) Specifies the well-known community by using the following keywords: **internet:** Specifies routes free to be advertised to all peers. **local-as:** Specifies not to send out of the local AS or sub-autonomous system of a confederation. **no-advertise:** Specifies not to advertise the route to other BGP peers. **no-export:** Specifies not advertise to external peers. Multiple number (separated by space) can be specified
additive	(Optional) Specifies to add the specified community to the existing communities.

Default

There is no set community statement.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

BGP community exchange is not enabled by default. It is enabled on a per-neighbor basis with the **neighbor send-community** command. The community will be sent out in the BGP packet only when **set community** is specified in the route map, and if all match criteria are met, all set actions are performed.

If **additive** is not specified, the user-defined communities in the route will be replaced.

This command is useful for routes received from eBGP and to be transmitted to iBGP.

You can verify your settings by entering the **show route-map** command.

Example

This example shows how to create a route map “myPolicy” which sets the community of routes that pass the AS path list, ACL1 to 0:1.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path ACL1
Switch(config-route-map)# set community 1:1
Switch(config-route-map)#
```

10-69 set dampening

This command is used to specify the dampening parameters of routes. Use the **no** form of this command to delete this set command.

set dampening *HALF-LIFE REUSE SUPPRESS MAX-SUPPRESS-TIME UN-REACHABILITY-HALF-LIFE*

no set dampening

Parameters

HALF-LIFE	Specifies the time (in minutes) after which the penalty of the reachable routes is decreased by half. The range is 1 to 45.
REUSE	Specifies that if the penalty of a route is lower than this value, the route is unsuppressed. The range is 1 to 20000
SUPPRESS	Specifies that if the penalty of a route is higher than this value, the route is suppressed. The range is 1 to 20000.
MAX-SUPPRESS-TIME	Specifies the maximum time (in minutes) a route can be suppressed. The range is 1 to 255.
UN-REACHABILITY-HALF-LIFE	Specifies the time (in minutes) after which the penalty of the unreachable routes is decreased by half. The range is 1 to 45.

Default

HALF-LIFE: 15 minutes.

REUSE: 750.

SUPPRESS: 2000.

MAX-SUPPRESS-TIME: 60 minutes.

UN-REACHABILITY-HALF-LIFE: 15 minutes.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to modify the dampening parameters of routes when match conditions are met.

Example

This example shows how to add a set command to modify the dampening parameters of route 120.1.1.0/24.

```
Switch# configure terminal
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 120.1.1.0 0.0.0.255
Switch(config-ip-acl)# exit
Switch(config)# route-map rmap1 permit 10
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set dampening 14 500 900 60 15
Switch(config-route-map)#
```

10-70 set metric

This command is used to set the MED value for the route matched by the route map. Use the **no** form of this command to remove setting of the MED value.

set metric *VALUE*

no set metric

Parameters

VALUE	Specifies the MED value, set for the matched route.

Default

There is no set metric statement.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

MED is an attribute specified by a local peer, and advertised to the remote peer to affect the best path selection result in the remote peer. The remote peer will not pass the MED value with routes for further path advertisement. The lower MED value is preferred than the larger MED value.

By default, the MED attribute only affects the selection of paths that are advertised by the same AS. Use the command **bgp always-compare-med** to enable the mechanism that uses the Multi Exit Discriminator (MED) in best path selection for paths that are advertised from neighbors in either the same or different AS.

To set the MED for a route advertised to a remote eBGP peer, specify the **set metric** command in a route map and apply the route map to the corresponding peer session. You can verify your settings by entering the **show route-map** command.

Example

This example shows how to set the metric of routes that pass the AS path list, PATH_ACL in the route map, named myPolicy, to 100.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set metric 100
Switch(config-route-map)#
```

10-71 set local-preference

This command is used to set the local preference for the routes matched by the route map. Use the **no** form of this command to remove the set entry.

set local-preference *VALUE*

no set local-preference

Parameters

VALUE	Specifies to set the local preference for the matched route.

Default

There is no set statement.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The local preference number is used to control the preferred exit point from the local AS to the same destination network. The local preference will be sent with the route advertised to the iBGP peers. If an external route is both learned via the local router and an iBGP peer router, the local preference value determines the preferred exit point to reach the external route.

Use the **bgp default local-preference** command to specify the default local preference to be associated with the routes received by the router from eBGP peers.

Example

This example shows how to set the local preference of routes that passes the AS path list, PATH_ACL in the route map, named myPolicy, to 80.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set local-preference 80
```

10-72 set origin

This command is used to set the BGP origin code. To delete an entry, use the **no** form of this command.

set origin {igp | egp | incomplete}

no set origin

Parameters

igp	Specifies that the prefix is originated from an Interior Gateway Protocol.
egp	Specifies that the prefix is originated from an Exterior Gateway Protocol.
incomplete	Specifies that the prefix is originated from an unknown source.

Default

The default origin follows the value in the main IP routing table.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The route redistribute to BGP has the origin code “INCOMPLETE”. The main purpose of this command is to set origin code for the redistributed route. The origin code (ORIGIN) is a well-known mandatory attribute that indicates the origin of the prefix.

The origin code has three values:

- IGP, indicates that the prefix is originated from an Interior Gateway Protocol.
- EGP, indicates that the prefix is originated from an Exterior Gateway Protocol.
- INCOMPLETE, indicates that the prefix is originated from unknown source.

You can verify your settings by entering the **show route-map** command.

Example

This example shows how to set the origin of routes that pass the AS path list, PATH_ACL in the route map, named myPolicy, to EGP.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set origin egp
```

10-73 set weight

This command is used to set the BGP weight for the matched routes. Use the **no** form of the command to remove the command statement.

set weight *NUMBER*

no set weight

Parameters

NUMBER	Specifies the weight for the matched routes. This value must be between 0 and 65535.

Default

There is no set weight statement.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

BPG weight is an attribute that is assigned by the local router to affect the best path selection on the local router among eBGP routes. The specified weight is associated with the inbound paths. The weight attribute will not be propagated with the route.

Weight can be specified per neighbor session by the **neighbor weight** command. The routes received from this session will be associated with this weight. The weight can also be set in route map to associate the weight with the ingress route. When a route's weight is set by both the **neighbor weight** command and the **set weight** command, the setting set by the **set weight** command will override the setting set by the **neighbor weight** command.

You can verify your settings by entering the **show route-map** command.

Example

This example shows how to define a route map myPolicy rule entry 1 to set the weight to 30 for the routes match the as-path access list PATH_ACL.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match as-path PATH_ACL
Switch(config-route-map)# set weight 30
```

10-74 show ip as-path access-list

This command is used to display the configured AS-path access-lists.

show ip as-path access-list [*ACCESS-LIST-NAME***]**

Parameters

ACCESS-LIST-NAME	(Optional) Specifies the AS path access list to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the configured AS-path access-lists. If the access list name is not specified, all as-path access-lists are displayed.

Example

This example shows how to display all of the configured AS path access list.

```
Switch#show ip as-path access-list

AS path access list A1
   permit .*

AS path access list A2
   permit .*

Total Entries: 2

Switch#
```

10-75 show ip bgp

This command is used to display entries in the Border Gateway Protocol (BGP) routing table.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] [***IP-ADDRESS* **[***IPREFIX-LENGTH* **[longer-prefixes]] | route-map** *NAME***]**

Parameters

ipv4	(Optional) Specifies to display the IPv4 address family routing entries.
vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries
unicast	Specifies to display unicast address family routing entries.
all	Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF_NAME*	Specifies to display the VPNv4 routing entries associated with the VRF.
IP-ADDRESS	(Optional) Specifies the IP network to display only a particular network in the BGP routing table.
PREFIX-LENGTH	(Optional) Specifies the length of prefix of the specified network.
longer-prefixes	(Optional) Specifies to display the specified route and all more specific routes.
NAME	(Optional) Specifies to filter the output based on the specified route map.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the routing entry information in BGP routing table. If a specific network is specified for the command, all the paths able to reach the network will be displayed. If a specific network is not specified for the command, all routes but only those best routes will be displayed. If no option is specified for the command, the entire routing table for IPv4 unicast address family is displayed.

Example

This example shows how to display the BGP routing table of IPv4 unicast address family. Only the best path is displayed in this general routing information display.

```
Switch# show ip bgp

BGP table version is 2, local router ID is 20.1.1.1
Status codes: s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

    Network        Next Hop      Metric      LocPrf   Weight  Path

*>  89.1.1.0/24   10.1.1.4          0                   0     5 i
*>  89.1.2.0/24   10.1.1.4          0                   0     5 i
*>  89.1.3.0/24   10.1.1.4          0                   0     5 i
*>  89.1.4.0/24   10.1.1.4          0                   0     5 i
*>  89.1.5.0/24   10.1.1.4          0                   0     5 i
*>  99.1.1.0/24   10.1.1.4          1           100     32768  i

Switch#
```

In the following example, all paths able to reach the specified route are displayed.

```
Switch# show ip bgp 10.1.1.0/24

BGP routing table entry for 89.1.1.0/24
Paths:(1 available, best #1, table: Default_IP_Routing_Table.)
Advertised to non peer-group peer: 10.1.1.3

  AS path is:5
  Next hop is:10.1.1.4 (40.217.0.2)
  Origin IGP, metric 0, localpref 100, external, best

Switch#
```

This example shows how to output from the **show ip bgp** command entered with the **route-map** keyword.

```
Switch(config)# show ip bgp route-map RMAS1

BGP table version is 2, local router ID is 20.1.1.1
Status codes: s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete
```

```
    Network          Next Hop      Metric      LocPrf   Weight  Path

*>  89.1.1.0/24   10.1.1.4          0                    0     5 i
*>  89.1.2.0/24   10.1.1.4          0                    0     5 i
*>  89.1.3.0/24   10.1.1.4          0                    0     5 i
*>  89.1.4.0/24   10.1.1.4          0                    0     5 i
*>  89.1.5.0/24   10.1.1.4          0                    0     5 i
*>  99.1.1.0/24   10.1.1.4          1           100      32768  i

Switch(config)#
```

Display Parameters

BGP table version	The version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the path. It can be one of the following values: i - Path originated from IGP. e - Entry originated from EGP. ? - Origin of the path is not clear.
Network	The IP address of a network.
Next Hop	The IP address of the next router to forward the packet.
Metric	The value of the inter-autonomous system metric.
LocPrf	The local preference value.
Weight	The weight of the route.
Path	The AS path to the destination network.

10-76 show ip bgp aggregate

This command is used to display aggregate entries in the BGP database.

show ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME*] **aggregate [***NETWORK-ADDRESS***]**

Parameters

ipv4 unicast	(Optional) Specifies to display an aggregate entry of the IPv4 unicast address family

vpnv4 vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of the VRF name is 12 characters.
NETWORK-ADDRESS	(Optional) Specifies the network address and the sub-network mask.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use the **show ip bgp aggregate** command to display aggregate entries created.

Example

This example shows how to display aggregate entries.

```
Switch# show ip bgp aggregate

Network Address    Options
------------------ ------------------
100.0.0.0/8        -
200.0.0.0/10       summary-only

Total Aggregate Address Number:  2

Switch#show ip bgp vpnv4 vrf VPN-A aggregate

Network Address  VRF-Name  Options
---------------  --------  -------
5.5.5.0/24       VPN-A      -
100.0.0.0/8      VPN-A      summary-only

Total Aggregate Address Number:  2

Switch#
```

10-77 show ip bgp cidr-only

This command is used to display the CIDR (classless inter-domain routing) routes.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] cidr-only**

Parameters

ipv4 unicast	(Optional) Specifies to display the IPv4 address family routing entries.
vpn4	(Optional) Specifies to display the VPNv4 address family routing entries.

all	(Optional) Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated with the VRF.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the CIDR routing entry information in the BGP routing table.

Example

This example shows how to display the CIDR routing entry information the BGP routing table.

```
Switch# show ip bgp cidr-only

BGP table version is 13, local router ID is 10.1.1.99
Status codes:s suppressed,d damped,h history,* valid,> best,i – internal
Origin codes: i – IGP, e – EGP, ? – incomplete

   Network          Next Hop      Metric LocPrf  Weight   Path

*>  10.10.10.0/24   172.16.10.1    0               300   10 i
*>  10.10.20.0/24   172.16.10.1    0               300   10 i
*   10.20.10.0/24   172.16.10.1    0       0       300   10 i
*dh 30.10.1.1/24    172.3.3.2      100     50      200   20 i

Switch#
```

Display Parameters

BGP table version	The version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the path. It can be one of the following values: i - Path originated from IGP. e - Path originated from EGP.

	? - Origin of the path is not clear.
Network	The IP address of a network.
Next Hop	The IP address of the next router to forward the packet.
Metric	The value of the inter-autonomous system metric.
LocPrf	The local preference value.
Weight	The weight of the route.
Path	The AS path to the destination network.

10-78 show ip bgp community

This command is used to display routes that belong to specified Border Gateway Protocol (BGP) communities.

show ip bgp {ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] community** *COMMUNITY* **[exact]**

Parameters

ipv4	(Optional) Specifies to display the IPv4 address family routing entries.
vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries.
unicast	Specifies to display unicast address family routing entries.
all	(Optional) Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated with the VRF.
COMMUNITY	Specifies the community as a 32-bit integer. It can be a user-specified number represented by AA:NN, where AA (AS number) is the upper part of the word and NN (community number, user-specified) is the lower part of the word. Multiple numbers (separated by space) can be specified. It can also be one of the following reserved community: **internet:** Specifies routes free to be advertised to all peers. **local-as:** Specifies not to send out of the local AS or sub autonomous system of a confederation. **no-advertise:** Specifies not to advertise the route to other BGP peers. **no-export:** Specifies not advertise to external peers.
exact	(Optional) Specifies that an exact match is required. All of the communities and only those communities specified must be present.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the routes that match the specified community string. If no option is specified for the command, the information for IPv4 unicast address family will be displayed.

Example

This example shows how to display the display the routes that match the 111:12345 community string.

```
Switch#show ip bgp ipv4 unicast community 111:12345

BGP table version is 716977, local router ID is 192.168.32.1
Status codes:s suppressed,d damped,h history,* valid,> best,i – internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network          Next Hop      Metric LocPrf  Weight   Path

*> 0.10.10.0/24     172.16.10.1  0               300      10 i
*> 10.10.20.0/24    172.16.10.1  0               300      10 i
*  10.20.10.0/24    172.16.10.1  0               300      10 i

Switch#
```

Display Parameters

BGP table version	The version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the path. It can be one of the following values: i - Path originated from IGP. e - Path originated from EGP. ? - Origin of the path is not clear.
Network	The IP address of a network.
Next Hop	The IP address of the next router IP address of the next router to forward the packet.
Metric	The value of the inter-autonomous system metric.
LocPrf	The local preference value.
Weight	The weight of the route.
Path	The AS path to the destination network.

10-79 show ip bgp confederation

This command is used to display the confederation configuration of BGP.

show ip bgp confederation

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the detail of the confederation configured.

Example

This example shows how to display the detail of the confederation configured.

```
Switch# show ip bgp confederation

BGP AS Number             : 65501
Confederation Identifier : 10
Confederation Peer       : 65502, 65503
Neighbor List:
 IP Address       Remote AS Number
 ---------------  --------------------
 10.1.1.1         65501
 172.18.1.1       65503
 192.168.1.1      65502

Switch#
```

10-80 show ip bgp community-list

This command is used to display routes that are permitted by the Border Gateway Protocol (BGP) community list.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] community-list** *COMMUNITY-LIST-NAME* **[exact-match]**

Parameters

ipv4	(Optional) Specifies to display the IPv4 address family routing entries.

vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries.
unicast	Specifies to display the unicast routing entries.
all	(Optional) Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated with the VRF.
COMMUNITY-LIST-NAME	Specifies the name of community list.
exact-match	(Optional) Specifies to display only routes that are exact match.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the routes that match the specified community list. If no option is specified for the command, the information for IPv4 unicast address family will be displayed.

Example

This example shows how to display the routes that match the Marketing community list.

```
Switch#show ip bgp community-list Marketing

BGP table version is 716977, local router ID is 192.168.32.1
Status codes:s suppressed,d damped,h history,* valid,> best,i – internal
Origin codes: i - IGP, e - EGP, ? – incomplete

  Network          Next Hop     Metric LocPrf  Weight Path

* i10.20.0.0       10.0.22.1    0      100     0      750 ?
*>i               10.0.16.1    0      100     0      750 ?
* i10.26.0.0       10.0.22.1    0      100     0      790 768 ?
*>i               10.0.16.1    0      100     0      790 768 ?
* i10.17.0.0       10.0.22.1    0      100     0      200 11  ?
*>i               10.0.16.1    0      100     0      201 11  ?
*                 10.92.72.24  0           1878      201 11  ?
* i10.23.0.0       10.0.22.1    0      100     0      790 100 ?
*>i               10.0.16.1    0      100     0      790 100 ?
*                 10.92.72.24  0           1878      200 100 ?
* i10.12.0.0       10.0.22.1    0      100     0      200 i
*>i               10.0.16.1    0      100     0      200 i
*                 10.92.72.24  0           1878      200 i

Switch#
```

Display Parameters

BGP table version	The version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the path. It can be one of the following values: i - Path originated from IGP. e - Path originated from EGP. ? - Origin of the path is not clear.
Network	The IP address of a network.
Next Hop	The IP address of the next router IP address of the next router to forward the packet.
Metric	The value of the inter-autonomous system metric.
LocPrf	The local preference value.
Weight	The weight of the route.
Path	The AS path to the destination network.

10-81 show ip bgp dampening dampened-paths

This command is used to display the dampened paths in the routing table.

show ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME***}] dampening dampened-paths**

Parameters

ipv4	(Optional) Specifies to display the IPv4 address family routing entries.
unicast	Specifies to display the unicast routing entries.
vrf *VRF-NAME*	Specifies to display the VRF address family routing entries.
vpnv4	Specifies to display the IPv4 VPN address family routing entries.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If no option is specified for the command, the information for IPv4 unicast address family will be displayed.

Example

This example shows how to display the dampened paths.

```
Switch# show ip bgp dampening dampened-paths

BGP table version is 13, local router ID is 10.1.1.99
Status codes:s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

   Network          From            Reuse           Path

*d 10.10.21.0/24    192.168.1.1     00:02:35        32768 i
*d 168.22.2.0/24    192.168.1.1     00:03:01        45000 i

Switch#
```

Display Parameters

BGP table version	The version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the path. It can be one of the following values: i - Path originated from IGP. e - Entry originated from EGP. ? - Origin of the path is not clear.
Network	The IP address of a network.
From	The router that advertise this dampened path
Reuse	The time after which the path will be recovered as normal.
Path	The AS path to the destination network.

10-82 show ip bgp dampening flap-statistics

This command is used to display BGP flap statistics.

show ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME***}] dampening flap-statistics**

Parameters

ipv4	(Optional) Specifies to display the IPv4 address family routing entries.
vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries.
unicast	Specifies to display the unicast routing entries.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated with the VRF.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to show flap entries in the BGP routing table. If no option is specified for the command, the information for IPv4 unicast address family will be displayed.

Example

This example shows how to show flap entries in the BGP routing table.

```
Switch# show ip bgp dampening flap-statistics

BGP table version is 1538, local router ID is 172.29.232.182
Status codes: s suppressed, d damped, h history, * valid, > best, i –internal
Origin codes: i - IGP, e - EGP, ? – incomplete

   Network       From             Flaps    Duration    Reuse      Path

*d 10.10.0.0/8    172.33.22. 77    6        00:15:41    00:28:10   100i
*d 10.20.0.0/16   172.339.22. 77   6        00:02:43    00:23:20   100i

Switch#
```

Display Parameters

BGP table version	The internal version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the entry. It can be one of the following values: i - Entry originated from IGP. e - Path originated from EGP.

	? - Origin of the path is not clear.
Network	The IP address of a network entity.
From	The IP address of the peer that advertised this path.
Flaps	The number of times the route has flapped.
Duration	The time since the router noticed the first flap.
Reuse	The time after which the path will be made available.
Path	The autonomous system path of the route that is being dampened.

10-83 show ip bgp dampening parameters

This command is used to display BGP dampening configurations.

show ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME***] dampening parameters**

Parameters

ipv4	(Optional) Specifies to display setting for the IPv4 address.
vpnv4	(Optional) Specifies to display setting for the VPNv4 address family.
unicast	Specifies to display setting for the unicast address family.
vrf *VRF-NAME*	Specify to display setting for the VRF address family.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display BPG dampening related setting. If no option is specified for the command, the information for IPv4 unicast address family will be displayed.

Example

This example shows how to display the dampening configuration information for the IPv4 unicast address family.

```
Switch# show ip bgp dampening parameters

BGP Dampening for IPv4 Unicast
----------------------------------------
BGP Dampening State             : Enabled

BGP Dampening Route Map         :
Half-life Time                  : 15 mins
Reuse Value                     : 750
Suppress Value                  : 2000
```

```
MAX Suppress Time               : 60 mins
Unreachable route's Half-life   : 15 mins

Switch#
```

10-84 show ip bgp filter-list

This command is used to display routes that conform to a specified AS path access list.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] filter-list** *ACCESS-LIST-NAME*

Parameters

ipv4	(Optional) Specifies the IPv4 address family. The type of address family determines the routing table that is displayed.
vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries.
unicast	Specifies to display the unicast routing information.
all	(Optional) Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated with the VRF.
ACCESS-LIST-NAME	Specifies an AS path access list and only the routes match the access list are displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the BGP routes that conform to a specific access list. If no option is specified for the command, the information for IPv4 unicast address family will be displayed.

Example

This example shows how to displays the BGP routes that conform to the AS path access-list, as-ACL-HQ.

```
Switch# show ip bgp filter-list as-ACL-HQ

BGP table version is 1738, local router ID is 172.16.72.24
Status codes: s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

   Network          Next Hop          Metric  LocPrf  Weight Path
```

```
*  172.16.0.0       172.16.72.30            0          108    ?
*  172.16.1.0       172.16.72.30            0          108    ?
*  172.16.11.0      172.16.72.30            0          108    ?
*  172.16.14.0      172.16.72.30            0          108    ?
*  172.16.15.0      172.16.72.30            0          108    ?
*  172.16.16.0      172.16.72.30            0          108    ?
*  172.16.17.0      172.16.72.30            0          108    ?
*  172.16.18.0      172.16.72.30            0          108    ?
*  172.16.19.0      172.16.72.30            0          108    ?
*  172.16.24.0      172.16.72.30            0          108    ?
*  172.16.29.0      172.16.72.30            0          108    ?
*  172.16.30.0      172.16.72.30            0          108    ?
*  172.16.33.0      172.16.72.30            0          108    ?
*  172.16.35.0      172.16.72.30            0          108    ?
*  172.16.36.0      172.16.72.30            0          108    ?
*  172.16.37.0      172.16.72.30            0          108    ?
*  172.16.38.0      172.16.72.30            0          108    ?
*  172.16.39.0      172.16.72.30            0          108    ?

Switch#
```

Display Parameters

BGP table version	The version number of the table. This number is incremented whenever the table changes.
local router ID	The IP address of the router.
Status codes	The status of the path. It can be one of the following values: s - The path is suppressed. d - The path is dampened. h - The entry is a history path. * - The path is valid. > - The entry is the best path to that network. i - The path was learned via an iBGP session.
Origin codes	The origin of the path. It can be one of the following values: i - Path originated from IGP. e - Entry originated from EGP. ? - Origin of the path is not clear.
Network	The IP address of a network.
Next Hop	The IP address of the next router that is used in forwarding a packet to the destination network.
Metric	The value of the inter-autonomous system metric.
LocPrf	The local preference value.
Weight	The weight of the route.
Path	The AS path to the destination network.

10-85 show ip bgp inconsistent-as

This command is used to display the routes which have the same prefix and different AS path origins.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] inconsistent-as**

Parameters

ipv4 unicast	(Optional) Specifies to display the IPv4 address family routing entries.
vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries.
all	(Optional) Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated with the VRF.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the routes which have inconsistent-as originating autonomous systems.

Example

This example shows how to display the routes which have inconsistent-as originating autonomous systems.

```
Switch# show ip bgp inconsistent-as

BGP table version is 1738, BGP Local Router ID is 10.90.90.10
Status codes:s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

   Network          Next Hop          Metric  LocPrf  Weight Path

*  172.16.1.0/24    172.16.72.30      0       109     108    i
                    172.16.72.21      0       110     101    i
*  172.16.11.0/24   172.16.72.30      0       109     108    i
                    172.16.72.10      0       104     105    i
                    172.16.72.10      0       104     103    i

Switch#
```

10-86 show ip bgp vpnv4 labels

This command is used to display the BGP private labels of the routes, which are assigned from MPLS.

show ip bgp vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***} labels**

Parameters

all	Specifies to display all the VPNv4 routes labels.
rd *RD-VALUE*	Specifies to display the VPNv4 routes labels that match the specified RD.
vrf *VRF-NAME*	Specifies to display the VPNv4 routes labels associated with the VRF.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the BGP private labels of the routes.

Example

This example shows how to display the BGP private labels of the routes that match the RD 1:1.

```
Switch# show ip bgp rd 1:1 labels

BGP table version is 1738, BGP Local Router ID is 11.11.11.11
Status codes:s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? - incomplete

Network          From       In Label/Out Label

Route Distinguisher: 1:1 (default for VRF my)
*> 88.1.2.0/24      100.1.1.2      1000/no
*> 88.1.5.0/24      100.1.1.2      1000/no
*> 89.1.1.0/24      10.1.1.3       no/16
*> 89.1.2.0/24      10.1.1.3       no/17
*> 99.1.1.0/24      Self Peer      1000/no
Route Distinguisher: 1:1 (VPN route(s))
*> 89.1.1.0/24      10.1.1.3       no/16
*> 89.1.2.0/24      10.1.1.3       no/17

Switch#
```

10-87 show ip bgp neighbors

This command is used to display information about the TCP and Border Gateway Protocol (BGP) connections to neighbors.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] neighbors [***IP-ADDRESS* **[advertised-routes | received prefix-filter | received-routes | routes]]]**

Parameters

ipv4	(Optional) Specifies the IPv4 address family. The type of address family determines the routing table that is displayed.
vpnv4	(Optional) Specifies the VPNv4 address family. The type of address family determines the routing table that is displayed.
unicast	Specifies to display the unicast routing information.
all	(Optional) Specifies to display all the VPNv4 neighbors.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 neighbors that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 neighbors that match the specified VRF.
IP-ADDRESS	(Optional) Specifies the IP address of a neighbor to be displayed. If not specified, all neighbors are displayed.
advertised-routes	(Optional) Specifies to display the routes advertised to a BGP neighbor.
received prefix-filter	(Optional) Specifies to display the prefix-list received from the specified neighbor.
received-routes	(Optional) Specifies to display the routes received from a BGP neighbor.
routes	(Optional) Specifies to display the routes that are received and accepted from a neighbor. The accepted routes are a subset of the received routes.

Default

None.

Command Mode

EXEC Mode or any configuration mode,

Command Default Level

Level: 1.

Usage Guideline

Use this command to display BGP and TCP connection information for neighbor sessions. You can specify the IPv4 address of a neighbor to display information about the specific neighbor. If no option is specified for the command, the BGP neighbor information for IPv4 unicast address family is displayed. To display the received routes from a neighbor, the BGP soft reconfigure command setting must be enabled first.

Example

This example shows how to display the general neighbor information using the **show ip bgp neighbors** command.

```
Switch# show ip bgp neighbors

BGP neighbor: 10.1.1.3, remote AS 1, internal link
  BGP version: 4, remote router ID: 40.217.0.1
  BGP state = Established, up for 00:24:52
```

```
  Last read: 00:00:08, last write: 00:00:08, hold time: 90,
      keepalive interval: 30
  Configured hold time: 180, keepalive interval: 60
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Byte AS number: advertised
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: advertised and received
  Received 52 messages, 0 notifications, 0 in queue
  Sent 56 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 5 seconds
  Minimum time between AS origination advertisement runs is 15 seconds

 For address family: IPv4 Unicast
  BGP table version 12, neighbor version 12
  Index 1, Offset 0, Mask 0x2
  0 accepted prefixes, maximum limit 12000
  Threshold for warning message 75%
  1 announced prefixes

 For address family: VPNv4 Unicast
  BGP table version 1, neighbor version 1
  Index 1, Offset 0, Mask 0x2
  Community attribute sent to this neighbor (extended)
  0 accepted prefixes, maximum limit 12000
  Threshold for warning message 75%
  1 announced prefixes

 Connections established 1; dropped 0
 Local host: 10.90.90.90, Local port: 179
 Foreign host: 10.1.1.3, Foreign port: 33334
 Nexthop: 10.90.90.90

BGP neighbor: 10.1.1.4, remote AS 5, external link
 Member of peer-group my for session parameters
  BGP version: 4, remote router ID: 40.217.0.2
  BGP state = Established, up for 00:24:47
  Last read: 00:00:09, last write: 00:00:09, hold time: 90,
      keepalive interval: 30
  Configured hold time: 180, keepalive interval: 60
  Neighbor capabilities:
    Route refresh: advertised and received (old and new)
    4-Byte AS number: advertised
    Address family IPv4 Unicast: advertised and received
    Address family VPNv4 Unicast: received
  Received 64 messages, 0 notifications, 0 in queue
  Sent 53 messages, 0 notifications, 0 in queue
  Route refresh request: received 0, sent 0
  Minimum time between advertisement runs is 30 seconds
  Minimum time between AS origination advertisement runs is 15 seconds

 For address family: IPv4 Unicast
  BGP table version 12, neighbor version 12
```

```
  Index 2, Offset 0, Mask 0x4
  my peer-group member
  5 accepted prefixes, maximum limit 12000
  Threshold for warning message 75%
  1 announced prefixes

 Connections established 1; dropped 0
 Local host: 10.90.90.90, Local port: 1025
 Foreign host: 10.1.1.4, Foreign port: 179
 Nexthop: 10.90.90.90

Switch#
```

This example shows how to display routes advertised to the 172.16.232.178 neighbor.

```
Switch# show ip bgp neighbors 172.16.232.178 advertised-routes

BGP table version is 27, local router ID is 172.16.232.181
Status codes: s suppressed,d damped,h history,* valid,> best,i – internal
Origin codes: i - IGP, e - EGP, ? - incomplete

   Network       Next Hop          Metric    LocPrf Weight  Path

*>i10.0.0.0      172.16.232.179         0    100         0      ?
*> 10.20.2.0     10.0.0.0               0            32768      i

Switch#
```

This example shows how to display a prefix-list that filters all routes in the 10.0.0.0 network has been received from the 192.168.20.72 neighbor.

```
Switch# show ip bgp neighbors 192.168.20.72 received prefix-filter

Address family:IPv4 Unicast
1 entries
   seq 5 deny 10.0.0.0/8 le 32

Switch#
```

10-88 show ip bgp network

This command is used to display networks created by BGP network.

show ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME***] network [***NETWORK-ADDRESS***]**

Parameters

ipv4 unicast	(Optional) Specifies to display aggregate entry of the IPv4 unicast address family
NETWORK-ADDRESS	Specifies the IP network address. If a specific network address is not

	specified, all IP addresses will be displayed.
vpnv4 vrf *VRF-NAME*	(Optional) Specifies a VRF name. The length of the VRF name is 12 characters.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the networks advertised by BGP.

Example

This example shows how to display the networks advertised by BGP.

```
Switch# show ip bgp network

Network Address  Route Map
--------------------------
20.0.0.0/24      -

Total Network Number:  1

Switch# show ip bgp vpnv4 vrf VPN-A network

Network Address  VRF-Name  Route Map
-----------------------------------
20.0.0.0/8       VPN-A     -

Total Network Number:  1

Switch#
```

10-89 show ip bgp parameters

This command is used to display the parameters of BGP.

show ip bgp parameters

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the parameters of BGP.

Example

This example shows how to display the parameters of BGP.

```
Switch# show ip bgp parameters

BGP Global State                    : Enabled
Version                             : 4
BGP Router Identifier               : 20.1.1.1
Synchronization                     : Disabled
Enforce First AS                    : Disabled
Local AS Number                     : 1
Scan Time                           : 60 Seconds
Hold Time                           : 180 Seconds
Keepalive Interval                  : 60 Seconds
Always Compare MED                  : Disabled
Deterministics MED                  : Disabled
Med Confed                          : Disabled
Default Local Preference            : 100
AS Path Ignore                      : Disabled
Compare Router ID                   : Disabled
MED Missing as Worst                : Disabled
Compare Confederation Path          : Disabled
Fast External Failover              : Enabled
Aggregate Next Hop Check            : Disabled
Default IPv4 Unicast                : Enabled

Switch#
```

10-90 show ip bgp peer-group

This command is used to display information about the peer group of BGP.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] peer-group [***PEER-GROUP-NAME***]**

Parameters

ipv4 unicast	(Optional) Specifies the IPv4 unicast address family.
vpnv4	(Optional) Specifies the VPNv4 unicast address family.
all	(Optional) Specifies to display all the VPNv4 peer-groups.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 peer-groups that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 peer-groups that match the specified VRF. The length of VRF-NAME is 12 characters.

PEER-GROUP-NAME	Specifies the name of a Border Gateway Protocol (BGP) peer group. The maximum length is 16 characters.

Default

None.

Command Mode

EXEC Mode or any configuration.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the contents of the BGP peer group.

Example

This example shows how to display the information of the peer group named mygroup.

```
Switch# show ip bgp peer-group mygroup

BGP peer-group is mygroup
  Configured hold time: 180, keepalive interval: 60
  BGP version 4
  Default minimum time between advertisement runs is 30 seconds
  Minimum time between AS origination advertisement runs is 15 seconds

 For address family: IPv4 Unicast
  BGP neighbor is mygroup, peer-group external, members:
  10.1.1.4
  Index 0, Offset 0, Mask 0x0
  Maximum-Prefix limit 12000
  Threshold for warning message 75%

Switch#
```

10-91 show ip bgp quote-regexp

This command is used to display routes matching the regular expression.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] quote-regexp** *REGEXP*

Parameters

ipv4 unicast	(Optional) Specifies to display the IPv4 address family routing entries.
vpnv4	(Optional) Specifies to display the VPNv4 address family routing entries.
all	(Optional) Specifies to display all the VPNv4 routing entries.
rd *RD-VALUE*	(Optional) Specifies to display the VPNv4 routing entries that match the specified RD.
vrf *VRF-NAME*	(Optional) Specifies to display the VPNv4 routing entries associated

	with the VRF.
REGEXP	Specifies to display routes matching the AS path regular expression. The maximum length is 80 characters.

Default

None.

Command Mode

EXEC Mode or any configuration.

Command Default Level

Level: 1.

Usage Guideline

Use this command displays the routes which matching the AS path regular expression.

Example

This example shows how to display the routes which matching the AS path regular expression.

```
Switch# show ip bgp quote-regexp “100”

BGP table version is 1738, BGP Local Router ID is 10.90.90.10
Status codes:s suppressed,d damped,h history,* valid,> best,i - internal
Origin codes: i - IGP, e - EGP, ? – incomplete

   Network          Next Hop          Metric  LocPrf  Weight Path

s  172.16.0.0/24       172.16.72.30 0   100                108 100 ?
s  172.16.0.0/24       172.16.72.30 0   100                108 100 ?
*  172.16.1.0/24       172.16.72.30 0   100                108 100 ?
*  172.16.11.0/24      172.16.72.30 0   100                108 100 ?
*  172.16.14.0/24      172.16.72.30 0   100                108 100 ?
*  172.16.15.0/24      172.16.72.30 0   100                108 100 ?
*  172.16.16.0/24      172.16.72.30 0   100                108 100 ?

Switch#
```

10-92 show ip bgp redistribute

This command is used to display the route redistribution configuration of BGP.

show ip bgp [ipv4 unicast | vpnv4 vrf *VRF-NAME*] **redistribute**

Parameters

ipv4 unicast	(Optional) Specifies the IPv4 unicast address family.
vpnv4 vrf *VRF-NAME*	(Optional) Specifies the VRF family. The type of address family determines the routing redistribution information that is displayed.

Default

None.

Command Mode

EXEC Mode or any configuration.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the route redistribution configuration about BGP. If no option is specified for the command, the route redistribution information for IPv4 unicast address family is displayed.

Example

This example shows how to check the route redistribution configuration about BGP.

```
Switch# show ip bgp redistribute

Route Redistribution Settings

Source    Destination  Type  Metric  RouteMapName
Protocol  Protocol
--------  ------------ ----  ------  ------------
LOCAL     BGP          All   0       N/A

Total Entries : 1

Switch#show ip bgp vpnv4 vrf VPN-A redistribute

Route Redistribution Settings (For VRF VPN-A)

Source    Destination  Type  Metric  RouteMapName
Protocol  Protocol
--------  ------------ ----  ------  ------------
LOCAL     BGP          All   0        N/A

Total Entries : 1

Switch#
```

10-93 show ip bgp reflection

This command is used to display the route reflection configuration of BGP.

show ip bgp [ipv4 unicast | vpnv4 unicast] reflection

Parameters

ipv4 unicast	(Optional) Specifies to display reflection information of the IPv4 address family.
vpnv4 unicast	(Optional) Specifies to display reflection information of the VPNv4 address family.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display what have been already configured to the local BGP about the route reflection.

Example

This example shows how to display what have been already configured to the local BGP about the route reflection.

```
Switch# show ip bgp reflection

  Client to Client Reflection State : Disabled
  Cluster ID                        : 0.0.0.0
  Route Reflector Client            :
  peer group: inter (172.18.10.1)
  172.18.10.3
  172.18.10.4
  172.18.10.5

Switch#
```

10-94 show ip bgp summary

This command is used to display BGP summary information.

show ip bgp [ipv4 unicast | vpnv4 {all | rd *RD-VALUE* **| vrf** *VRF-NAME***}] summary**

Parameters

ipv4	(Optional) Specifies the IPv4 address family. The type of address family determines the routing table that is displayed.
unicast	Specifies to display the unicast address family.
vrf *VRF-NAME*	(Optional) Specifies the VRF family. The type of address family determines the routing table that is displayed.
vpnv4	(Optional) Specifies the IPv4 VRF family. The type of address family determines the routing table that is displayed.
all	(Optional) Specifies to display summary information for all the VPNv4 address family.
rd *RD-VALUE*	(Optional) Specifies to display summary information associated with the RD.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the BGP information by summary. If no option is specified for the command, the BGP summary information for IPv4 unicast address family is displayed.

Example

This example shows how to display BGP summary information.

```
Switch# show ip bgp summary

BGP router identifier 20.1.1.1, local AS number 1
BGP table version is 2, main routing table version 2

Neighbor   Ver AS      MsgRcvd    MsgSent    Up/Down     State/PfxRcd
---------- --- ------- ---------- ---------- ----------- -----------
10.1.1.3    4   1          27         30         00:12:28        0
10.1.1.4    4   5          28         27         00:12:21        5
10.10.10.10 4   1          0          0          never         Connect

Total Number of Neighbors: 3

Switch#
```

Display Parameters

Neighbor	The IPv4 address of the neighbor.
Ver	The version of BGP used to talk to the neighbor.
AS	The neighbor's autonomous number.
MsgRcvd	The number of received messages.
MsgSent	The number of sent messages.
Up/Down	The length of time that the neighbor session is in the state.
State/PfxRcd	This will display "Idle" if the session is terminated due to reaching the maximum prefix. It will display "Idle (Admin)" if the session is shutdown by the command. Otherwise, it display the number of received prefixes.

10-95 show ip community-list

This command is used to display the configured community lists.

show ip community-list [*COMMUNITY-LIST-NAME***]**

Parameters

COMMUNITY-LIST-NAME	(Optional) Specifies the community list name. The community list name can be standard or expanded.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display a specific community list or all configured community lists.

Example

This example shows how to display all of the configured IP community lists.

```
Switch# show ip community-list

Standard community list C1
  permit internet

Standard community list C2
  permit internet

Total Entries: 2

Switch#
```

10-96 show ip extcommunity-list

This command is used to display the configured extended community lists.

show ip extcommunity-list [*EXTCOMMUNITY-LIST-NAME***]**

Parameters

EXTCOMMUNITY-LIST-NAME	(Optional) Specifies the extended community list name. The community list name can be standard or expanded.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display a specific extended community list or all configured extended community lists.

Example

This example shows how to display all of the configured IP extended community lists.

```
Switch# show ip extcommunity-list

Expanded extended community list e1
       permit : _23

Standard extended community list s1
       permit : RT  1:1
SoO 1.1.1.1:1
       permit : SoO 2:3 3.2.1.1:10

Total Entries: 2

Switch#
```

10-97 snmp-server enable traps bgp

This command is used to enable Border Gateway Protocol (BGP) support for Simple Network Management Protocol (SNMP) operations. Use the **no** form of this command to disable it.

snmp-server enable traps bgp {established | backward-trans}

no snmp-server enable traps bgp {established | backward-trans}

Parameters

established	Specifies to enable or disable the sending of the peer established trap.
backward-trans	Specifies to enable or disable the sending of the peer idle trap.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the BGP trap state.

Example

This example shows how to enable the sending of the BGP peer established trap.

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

10-98 synchronization

This command is used to enable the advertisement of a route to an external neighbor by the BGP speaker unless the route is a local router or the BGP speaker has learned the route by IGP. Use the **no** form of this command to disable the option.

synchronization

no synchronization

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When synchronization is enabled, the BGP speaker will not advertise a route to an external neighbor unless the route is a local route or the BGP speaker has learned the route by IGP.

Example

This example shows how to enable synchronization for the BGP process.

```
Switch# configure terminal
Switch(config)# router bgp 65121
Switch(config-router)# synchronization
Switch(config-router)#
```

10-99 timers bgp

This command is used to configure BGP network timers. Use the **no** form of this command to restore the default setting.

timers bgp *KEEP-ALIVE HOLD-TIME*

no timers bgp

Parameters

KEEP-ALIVE	Specifies the interval that the software sends keep-alive messages to its BGP peer. The range is from 0 to 65535.
HOLD-TIME	Specifies the length of the time-out value of the keep-alive message. The software will declare a BGP peer dead after the timeout. The range is from 0 to 65535.

Default

KEEP-ALIVE: 60 seconds.

HOLD-TIME: 180 seconds.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The suggested default value for the keep-alive value is a third of the hold-time value. The user can configure the timers for all BGP neighbors using the **timers bgp** command or configure the timers for a specific neighbor or peer group using the **neighbor timers** command. The timer configured for a specific neighbor overrides the timers configured for all BGP neighbors. If the minimum acceptable hold-time is configured, the BGP session will only be established when the remote peer is equal to or greater than the minimum hold time.

Example

This example shows how to change the keep-alive timer value to 50 seconds, the hold-time timer value to 150 seconds and the minimum acceptable hold-time value is 20 seconds.

```
Switch# configure terminal
Switch(config)# router bgp 65100
Switch(config-router)# timers bgp 50 150
```

10-100 debug ip bgp

This command is used to turn on the BGP debug function. Use the **no** form of this command to turn off the BGP debug function.

debug ip bgp

no debug ip bgp

Parameters

None.

Default

By default, BGP debug function is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on the BGP debug function while the global debug function has been turned on before.

Example

This example shows how to turn on the BGP debug function.

```
Switch# debug ip bgp
Switch#
```

10-101 debug ip bgp fsm-event

This command is used to turn on the BGP FSM event debug switch option. Use the **no** form of this command to turn off the BGP FSM event debug switch option.

debug ip bgp fsm-event

no debug ip bgp fsm-event

Parameters

None.

Default

By default, the BGP FSM event debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on the BGP FSM event debug switch option. When the BGP FSM event happens, debug information will be print if the BGP debug function is turned on. Use the command **debug ip bgp** to turn on BGP debug function.

Example

This example shows how to turn on the BGP FSM event debug switch option.

```
Switch# debug ip bgp fsm-event
Switch#
10.1.1.4-Outgoing [FSM] AS-Origination Timer Expiry
33.33.33.33-Outgoing [FSM] Routeadv Timer Expiry
10.1.1.3-Outgoing [FSM] Routeadv Timer Expiry
100.1.1.2-Outgoing [FSM] Routeadv Timer Expiry
100.1.1.2-Outgoing [FSM] Keep-alive-Timer Expiry
100.1.1.2-Outgoing [FSM] AS-Origination Timer Expiry
100.1.1.4-Outgoing [FSM] AS-Origination Timer Expiry
33.33.33.33-Outgoing [FSM] AS-Origination Timer Expiry
33.33.33.33-Outgoing [FSM] Routeadv Timer Expiry
```

10-102 debug ip bgp packet

This command is used to turn on the BGP packet debug switch option. Use the **no** form of this command to turn off the BGP packet debug switch option.

debug ip bgp packet {receive | send}

no debug ip bgp packet {receive | send}

Parameters

receive	Specifies to turn on the BGP received packet debug switch option.
send	Specifies to turn on the BGP sent packet debug switch option.

Default

By default, the BGP packet debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on the BGP packet debug switch option. When BGP protocol packets are received or transmitted, debug information will be print if the BGP debug function is turned on. Use the command **debug ip bgp** to turn on the BGP debug function.

Example

This example shows how to turn on the BGP received packet debug switch option.

```
Switch# debug ip bgp packet receive
Switch#
BGP:Peer:<100.1.1.2>,RCV UPDATE,withdraw,NLRI:<88.1.1.0/24>,<88.1.2.0/24>,<88.1.
3.0/24>,<88.1.4.0/24>,<88.1.5.0/24>
100.1.1.2-Outgoing [DECODE] Update: Withdrawn Len(20)
100.1.1.2-Outgoing [RIB] Withdraw: Prefix 88.1.1.0
BGP:Peer:<10.1.1.3>,RCV KEEPAVLIVE
10.1.1.3-Outgoing [DECODE] KAlive: Received!
BGP:Peer:<100.1.1.2>,RCV UPDATE,attr:<Orign:i,As-path:(null),Next-hop:100.1.1.2>
,NLRI:<88.1.1.0/24>,<88.1.2.0/24>,<88.1.3.0/24>,<88.1.4.0/24>,<88.1.5.0/24>
100.1.1.2-Outgoing [DECODE] Update: NLRI Len(20)
100.1.1.2-Outgoing [RIB] Update: Received Prefix 88.1.1.0
```

10-103 debug ip bgp route-map

This command is used to turn on the BGP route map debug switch option. Use the **no** form of this command to turn off the BGP route map debug switch option.

debug ip bgp route-map

no debug ip bgp route-map

Parameters

None.

Default

By default, the BGP route map debug switch option is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on the BGP route map debug switch option. When the route map matches the BGP route information, debug information will be printed if the BGP debug function is turned on. Use the command **debug ip bgp** to turn on the BGP debug function.

Example

This example shows how to turn on the BGP route map debug switch option.

```
Switch# debug ip bgp route-map
Switch#
Route-Map:<you>, Apply Suppressed Route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<67.1.1.0/24> <Permit>
Route-Map:<my>, Apply Received route, Neighbor <100.1.1.2, AFI/SAFI 1/1>,Prefix:
<88.1.1.0/24> <Deny>
```

10-104 debug ip bgp prefix-list

This command is used to turn on the BGP IP prefix list debug switch option. Use the **no** form of this command to turn off the BGP IP prefix list debug switch option.

debug ip bgp prefix-list

no debug ip bgp prefix-list

Parameters

None.

Default

By default, the BGP IP prefix list debug switch option is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on the BGP IP prefix list debug switch option. When the IP prefix list matches the BGP information, debug information will be printed if the BGP debug function is turned on. Use the command **debug ip bgp** to turn on the BGP debug function.

Example

This example shows how to turn on the BGP IP prefix list debug switch option.

```
Switch# debug ip bgp prefix-list
Switch#
Prefix-List:<my>, Apply Received route, Neighbor <100.1.1.2, AFI/SAFI 1/1>,
Prefix:<88.1.1.0/24> <Permit>
```

```
Prefix-List: ORF Apply Sent route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<88.1.1.0/24> <Deny>
Prefix-List:<my>, Apply Received route, Neighbor <100.1.1.2, AFI/SAFI 1/1>,
Prefix:<88.1.2.0/24> <Deny>
Prefix-List: ORF Apply Sent route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<67.1.1.0/24> <Permit>
Prefix-List: ORF Apply Sent route, Neighbor <100.1.1.4, AFI/SAFI 1/1>,
Prefix:<67.1.2.0/24> <Deny>
```

10-105 debug ip bgp show global

This command is used to display internal detailed information about BGP.

debug ip bgp show global [vrf *VRF-NAME* **| vpnv4]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.
vpnv4	(Optional) Specifies to display global parameters in the address family of VPNv4.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check internal status and detailed information of BGP. If there is no parameter specified, then IPv4 global information will be displayed. If the parameter is VRF, followed by a VRF name, VRF global information will be displayed. If the parameter is VPNv4, then VPNv4 address family global information will be displayed.

Example

This example shows how to display detailed internal information about the IPv4 address family BGP.

```
Switch# debug ip bgp show global

Following is the information for global debugging:

AS Number : 1
Router ID : 10.2.2.2
Cluster ID : 30.1.1.1
Confed ID : 10
Confederation Peers : 65510 65511
Fast External Fallover : Disabled
Dampening Ability : Enable
Client to Client Ability : Enable
Cluster Peers :
```

```
1.1.1.2 group1
Aggregate Next_Hop_Check : Disabled
Default Local PREF : 100
Default HoldTime : 180
Default Keepalive : 60
Scan Time : 60

BGP Active Flags:
BGP_CFLAG_COMPARE_ROUTER_ID
BGP_CFLAG_ASPATH_IGNORE

BGP Active AF-Flags :  None
Note: The address family is IPv4

BGP Active Redist-Flags:
Note: The address family is IPv4

Switch#
```

10-106 debug ip bgp show neighbors

This command is used to display internal detailed information about BGP neighbors.

debug ip bgp show neighbors [vrf *VRF-NAME* **| vpnv4]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.
vpnv4	(Optional) Specifies to display global parameters in the address family of VPNv4.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of BGP neighbors.

Example

This example shows how to display internal detailed information about BGP neighbors.

```
Switch# debug ip bgp show neighbors

BGP neighbor: 10.1.1.3 (Internel Peer)
------------------------------------------------
Session State : Enabled
```

```
Session Activity : Enabled
Peer Group : my
Remote AS : 1
Local AS : 1
Remote Router ID : 182.148.0.3
BGP State : Established (UP for 00:21:48)
Hold Time (Configured) : 180 Seconds
Hold Time  (Current Used) : 90 Seconds
Keepalive Interval (Configured) : 60 Seconds
Keepalive Interval (Current Used) : 30 Seconds
Advertisement Interval (Configured) : 0 Seconds
Advertisement Interval (Current Used) : 5 Seconds
AS Origination Interval (Configured) : 0 Seconds
AS Origination Interval (Current Used) : 15 Seconds
Connect Retry Interval (Configured) : 0 Seconds
Connect Retry Interval (Current Used) : 0 Seconds
EBGP Multihop : 255
Weight : 0
Update Source : loopback1
Next Hop Self : Disabled
Remove Private As : Disabled
Allowas In : Disabled
Address Family IPv4 Unicast
IPv4 Unicast : Advertised and Received
Soft Reconfiguration Inbound : Disabled
Community Sent to this Neighbor : None
Default Originate : Disabled
Outbound Route Filter (ORF) type (64) Prefix list:
        Send Mode : Disabled
        Receive Mode : Disabled
Pass Word: (null)
Prefix Count: 0
Send Prefix Count: 1
Prefix Max Count: 12000
Prefix Warning Threshold: 75
Prefix Max Warning: Disabled

Switch#
```

10-107 debug ip bgp show peer-group

This command is used to display internal detailed information about the BGP peer group.

debug ip bgp show peer-group [vrf *VRF-NAME* **| vpnv4]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.
vpnv4	(Optional) Specifies to display global parameters in the address family

of VPNv4.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of a BGP peer group.

Example

This example shows how to display internal detailed information about a BGP peer group:

```
Switch# debug ip bgp show peer-group

BGP Peer Group :local1
------------------------------------------------------
Session State : Enabled
Session Activity : Enabled
Members : 10.1.1.3
Remote AS : Not Set
Holdtime Interval : 180 seconds
Keepalive Interval : 60 seconds
Advertisement Interval : 0 seconds
AS Origination Interval : 0 Seconds
Connect Retry Interval : 0 Seconds
EBGP Multihop : 255
Weight : 0
Update Source : loopback1
Next Hop Self : Disabled
Remove Private As : Disabled
Allowas In : Disabled
Soft Reconfiguration Inbound : Disabled
Community Sent to this Neighbor : None
Default Originate : Disabled
Capability ORF Prefix List : None
Pass Word:
Prefix Max Count: 12000
Prefix Warning Threshold: 75
Prefix Max Warning: Disabled

Switch#
```

10-108 debug ip bgp show network

This command is used to display internal detailed information about the BGP network.

debug ip bgp show network [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.

Default

None.

Command Mode

Privileged EXEC Mode or any configuration mode/

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of a BGP network.

Example

This example shows how to display internal detailed information about the BGP network of the address family of IPv4.

```
Switch# debug ip bgp show network

Network        Route Map
-------------  -----------
192.168.0.0/16 -
172.16.0.0/16  map1

Total Entries :2

Switch# debug ip bgp show network vrf vrf-1

Network        Route Map
-------------  -----------
172.16.0.0/16  map1

Total Entries :1

Switch#
```

10-109 debug ip bgp show aggregate

This command is used to display internal detailed information about BGP route aggregation.

debug ip bgp show aggregate [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of BGP route aggregation.

Example

This example shows how to display internal detailed information about BGP route aggregation.

```
Switch# debug ip bgp show aggregate

Network        Summary Only  AS Set  SuppressCount
-------------  ------------  ------  ------------
192.168.0.0/16 YES           NO      0
172.16.0.0/16  NO            NO      2

Total Entries :2

Switch# debug ip bgp show aggregate vrf vrf-1

Network        Summary Only  AS Set  SuppressCount
-------------  ------------  ------  ------------
50.0.0.0/8     NO            NO      0
60.0.0.0/8     NO            NO      0

Total Entries :2

Switch#
```

10-110 debug ip bgp show damp

This command is used to display internal detailed information about BGP route damping.

debug ip bgp show damp [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of BGP route damping.

Example

This example shows how to display internal detailed information about BGP route damping of the address family of IPv4.

```
Switch# debug ip bgp show damp

Route Map : NULL
Reach Half Life Time : 900 seconds
Reuse Value : 750
Suppress Value : 2000
Max Suppress Time : 3600 seconds
Unreach Half Life Time : 900 seconds
Reuse Index Size : 1024
Reuse List Size : 256
Reuse Offset : 19

Current dampened routes:
Damp Hinfo: 484d9be8
 index ptr  event  penalty binfo     rn
  f5   484d9be8  1 1392    484d9ad8  484d9a90
  f5   484d9b98  1 1392    484d9a00  484d99b8
  f5   484d8080  1 1392    484d9928  484d98e0
  f5   484d7fe8  1 1392    484d9808  484d9738
 Damp Reuse List Info:
reuse_index index ptr penalty flap start_time t_updated suppress_time evt
245         1  484d9be8 5010  6   428        448      437           1
245         2  484d9b98 5010  6   428        448      437           1
245         3  484d8080 5010  6   428        448      437           1
245         4  484d7fe8 5010  6   428        448      437           1

show BGP Damp  no reuse list info: 0
index ptr penalty flap  start_time  t_updated  suppress_time evt

BGP Damp Decay List Info:
decay array size is 90.
Index  value
-----------
1      1
2      0.969663
3      0.940247
4      0.911722
5      0.884064
6      0.857244
7      0.831238

Output truncated...

Switch#
```

10-111 debug ip bgp show interface

This command is used to display internal detailed information about the BGP interface.

debug ip bgp show interface

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of the BGP interface.

Example

This example shows how to display internal detailed information about the BGP interface.

```
Switch# debug ip bgp show interface

Interface Information:
Name      index  network       Flags  Status  VRF
------    -----  ---------     -----  ------  ------------
System    0001   10.1.1.2/24     5     Up       None
if3       0002   30.1.1.5/8      5     Up       None
if10      0003   100.1.1.1/8     5     Up       VPNA
if11      0004   10.1.1.1/8      5     Up       VPNB
if2       0005   44.1.1.21/8     5     Down     None
loopback1 0267   11.11.11.11/32  d     Up       None

Switch#
```

10-112 debug ip bgp show timer

This command is used to display internal detailed information about the BGP timer.

debug ip bgp show timer

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of the BGP timer.

Example

This example shows how to display internal detailed information about the BGP timer.

```
Switch# debug ip bgp show timer

BGP timer Link:
Node       Time   Func
--------  ------  --------
481f9ef8  1  80ca052c
480f4410  1  80ca052c
48135368  1  80ca052c
481760c8  1  80ca052c
481b6e28  1  80ca052c
481f7b88  1  80ca052c
481fdf14  1  80c98f34
481f9f14  1  80ca0710
480f442c  1  80ca0710
48135384  1  80ca0710
481760e4  1  80ca0710

Switch#
```

10-113 debug ip bgp show redistribution

This command is used to display internal detailed information about BGP route redistribution.

debug ip bgp show redistribution [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF name. This name can be up to 12 characters long.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of BGP route redistribution.

Example

This example shows how to display internal detailed information about BGP route redistribution.

```
Switch# debug ip bgp show redistribution

Redistributed routes summary:
Network      Type   Next_hop
-------      ----   -------------
10.0.0.0/8   LOCAL  0.0.0.0
21.0.0.0/24  RIP    10.2.2.2
21.0.1.0/24  RIP    10.2.2.2
21.0.2.0/24  RIP    10.2.2.2
21.0.3.0/24  RIP    10.2.2.2
21.0.4.0/24  RIP    10.2.2.2

Total Entries: 6

Redist list information:
No redist list exist!

Switch#
```

10-114 debug ip bgp show as-path-access-list

This command is used to display internal detailed information about the BGP path access list.

debug ip bgp show as-path-access-list

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of the BGP path access list.

Example

This example shows how to display internal detailed information about the BGP path access list.

```
Switch# debug ip bgp show as-path-access-list

BGP AS Path Access List 1
```

```
deny (_64[6-9][0-9][0-9]_|_65[0-9][0-9][0-9]_)
permit 33

Total Entries: 1

Switch#
```

10-115 debug ip bgp show community-list

This command is used to display internal detailed information about the BGP community list.

debug ip bgp show community-list

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check the internal status and detailed information of the BGP community list.

Example

This example shows how to display internal detailed information about the BGP community list.

```
Switch# debug ip bgp show community-list

Community list:list1  standard
    permit   5000:100

Switch#
```

11. BPDU Protection Commands

11-1 spanning-tree bpdu-protection (global)

This command is used to enable the BPDU protection function globally. Use the **no** form of this command to return to the default setting.

spanning-tree bpdu-protection

no spanning-tree bpdu-protection

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In a network, customers do not want all ports of devices to receive STP packets, because some ports that receive STP BPDU packets will cause system resources to be wasted.

If ports are not expected to receive BPDU packets, the BPDU protection function will prevent those ports from receiving BPDU packets. The port where the BPDU protection function is enabled will enter a protection state (drop/block/shutdown) when it receives a STP BPDU packet.

There are 3 mode behaviors when the switch detects BPDU attacks:

- Drop – The switch drops received STP BPDU packets only and the port is placed in the normal state.
- Block – The switch drops all received BPDU packets and bock all data and the port is placed in the normal state.
- Shutdown – The switch shuts down the port and the port is placed the error-disabled state.

Example

This example shows how to enable the BPDU protection function globally.

```
Switch# configure terminal
Switch(config)# spanning-tree bpdu-protection
Switch(config)#
```

11-2 spanning-tree bpdu-protection (interface)

This command is used to enable the BPDU protection function on a port. Use the **no** form of this command to disable the BPDU protection function on the port.

spanning-tree bpdu-protection {drop | block | shutdown}

no spanning-tree bpdu-protection

Parameters

drop	Specifies to drop all received BPDU packets when the interface enters the attacked state.
block	Specifies to drop all packets (include BPDU and normal packets) when the interface enters the attacked state.
shutdown	Specifies to shut down the interface when the interface enters the attacked state.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable and configure the BPDU protection operational mode. This command is available for the port and port channel interface configuration.

Example

This example shows how to enable the BPDU Protection function with block mode on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree bpdu-protection block
Switch(config-if)#
```

11-3 show spanning-tree bpdu-protection

This command is used to display BPDU protection information.

show spanning-tree bpdu-protection [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	Specifies the interface's ID to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display BPDU protection information. If no interface ID is specified, all interfaces' information will be displayed.

Example

This example shows how to display the BPDU protection information and status of interfaces.

```
Switch# show spanning-tree bpdu-protection

Global State:      Enabled

Interface           State           Mode           Status
--------------     --------       --------      ------------
eth1/0/1             Enabled        Shutdown      Under Attack
eth1/0/2             Enabled        Drop           Normal
eth1/0/3             Disabled       Block          -
…
port-channel1       Enabled        Shutdown      Under Attack

Switch#
```

This example shows how to display the BPDU protection status of interface eth1/0/1.

```
Switch# show bpdu-protection interface eth1/0/1

Interface             State           Mode           Status
---------------     --------       --------      ------------
eth1/0/1              Enabled        Shutdown      Under Attack

Switch#
```

This example shows how to display the BPDU protection status of interface port-channel 1.

```
Switch# show bpdu-protection interface port-channel 1

Interface           State           Mode           Status
--------------     --------       --------      ------------
port-channel1      Enabled        Shutdown      Under Attack

Switch#
```

Display Parameters

Interface	Indicates the interface that has BPDU protection enabled.
State	Indicates the interface's configuration state.
Mode	Indicates the operation mode of the interface.
Status	Indicates if the interface is under the protection state.

12. Cable Diagnostics Commands

12-1 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 separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is available for physical port 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 eth1/1/1
Switch#
```

12-2 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's ID. The acceptable interface will be a physical port.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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)
------  ----------  -------------  -------------------------------  -----------------
eth1/1/1     1000BASE-T  Link Up        OK                              65
eth1/1/2     1000BASE-T  Link Up        OK                               -
eth1/1/3     1000BASE-T  Link Down      Shutdown                        25
eth1/1/4     1000BASE-T  Link Down      Shutdown                         -
eth1/1/5     1000BASE-T  Link Down      Unknown                          -
eth1/1/6     1000BASE-T  Link Down      Pair 1 Crosstalk at  30M        -
                                       Pair 2 Crosstalk at  30M
                                       Pair 3 OK         at 110M
                                       Pair 4 OK         at 110M
eth1/1/7     1000BASE-T  Link Down      NO Cable                         -
eth1/1/8     1000BASE-T  Link Down      Pair 1 Open       at  16M       -
                                       Pair 2 Open       at  16M
                                       Pair 3 OK         at  50M
                                       Pair 4 OK         at  50M

Switch#
```

12-3 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's ID. The acceptable interface will be a physical port.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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 eth1/1/1
Switch#
```

13. Command Logging Commands

13-1 command logging enable

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

command logging enable

no command logging enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

The command logging function is used to log the commands that have successfully been configured to the switch via the command line interface. The requirement is to log the command itself, along with information about the user account that entered the command into the system log. Commands that do not cause a change in the switch configuration or operation (such as **show**) will not be logged. Information about saving or viewing the system log is described in the sys-log functional specification.

Note: When the switch is under the BAT process (booting procedure, execute downloaded configuration files, etc...), all configuration commands will not be logged.

Example

This example shows how to enable the command logging function.

```
Switch# configure terminal
Switch(config)# command logging enable
Switch(config)#
```

14. Connectivity Fault Management (CFM) Commands

14-1 ais

This command is used to configure the parameters of the Alarm Indication Signal (AIS) function. To disable the AIS function, use the **no** command.

ais [period *PERIOD***] [level** *LEVEL***]**

no ais [period | level]

Parameters

period *PERIOD*	(Optional) Specifies the transmitting interval of the AIS Protocol Data Unit (PDU). The default period is 1 second. It can be either 1second or 1 minute.
level *LEVEL*	(Optional)Specifies the client level ID to which the Maintenance association End Point (MEP) sends the AIS PDU. The default client Maintenance Domain (MD) level is that the most immediate client layer Maintenance domain Intermediate Points (MIP) and MEPs exist on. The range is from 0 to 7.

Default

By default, this option is disabled.

The default period is 1 second.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the parameters of the AIS function on a MEP. If no defined parameter, it will enable the CFM AIS function. This default client maintenance domain level is not a fixed value. It may change when creating or deleting a higher level maintenance domain and MA on the device.

Upon detecting a defect condition the MEP can immediately start transmitting periodic frames with ETH-AIS information at a configured client level. A MEP continues to transmit periodic frames with ETH-AIS information until the defect condition is removed. Upon receiving a frame with ETH-AIS information from its server (sub) layer, a client (sub) layer MEP detects AIS condition and suppresses alarms associated with all peer MEPs. A MEP resumes alarm generation upon detecting defect conditions once AIS condition is cleared

When the most immediate client layer MIPs and MEPs do not exist, the default client maintenance domain level cannot be calculated. If the default client maintenance domain level cannot be calculated and the user does not designate a client level, the AIS PDU cannot be transmitted.

Example

This example shows how to configure the AIS function so that it has a client level of 5.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
```

```
Switch(config-cfm-mep)# ais level 5
Switch(config-cfm-mep)#
```

14-2 alarm-time

This command is used to define the time period to control when a fault alarm will be sent if a defect is reported continuously and the time period to control when a fault alarm will be reset. Use the **no** form of the command to reset to the default setting.

alarm-time {delay *CENTISECOND* **| reset** *CENTISECOND***}**

no alarm-time {delay | reset}

Parameters

delay *CENTISECOND*	Specifies the time period to control when a fault alarm will be sent if a defect is reported continuously. The unit is centiseconds. The range is from 250 to 1000.
reset *CENTISECOND*	Specifies the time period to reset the fault alarm if a defect has not been reported since the last defect report. The unit is centiseconds. The range is from 250 to 1000.

Default

The default value of the MEP alarm delay time is 250.

The default value of the MEP alarm reset time is 1000.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command defines the time period to control when a fault alarm will be sent if a defect is reported continuously. This command also defines the time period to reset the fault alarm if a defect has not been reported since the last defect report.

Example

This example shows how to configure an MEP alarm time. Assign the alarm time of the MEP to 250.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# alarm-time delay 250
Switch(config-cfm-mep)#
```

This example shows how to configure an MEP alarm reset time. Assign the alarm reset time of the MEP to 1000.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# alarm-time reset 1000
```

```
Switch(config-cfm-mep)#
```

14-3 ccm enable

This command is used to enable the CFM Continuity Check Message (CCM) function. To disable this function, use the **no** command.

ccm enable

no ccm enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable the CFM CCM function.

Example

This example shows how to enable the CFM CCM function.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# ccm enable
Switch(config-cfm-mep)#
```

14-4 ccm interval

This command is used to configure the CCM interval for a Maintenance Association (MA). Use the **no** form of the command to reset to the default setting.

ccm interval *INTERVAL*

no ccm interval

Parameters

INTERVAL	Specifies the CCM interval. It can be one of the following values. **100 ms:** 100 milliseconds. It is not recommended in CFM software mode as it may exhaust CPU utilization. **1sec:** One second.

	10sec: Ten seconds. This is the default value. **1min:** One minute. **10min:** Ten minutes.

Default

By default, this value is 10 seconds.

Command Mode

CFM MA Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the CCM interval for an MA. An MEP will transmit a CCM packet periodically across the MA. The CCM interval indicates the interval at which CCMs are sent by a MEP in a MA.

Example

This example shows how to configure the CCM interval for an MA.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op1 vlan 2
Switch(config-cfm-ma)# ccm interval 10sec
Switch(config-cfm-ma)#
```

14-5 cfm domain

This command is used to define an MD. To delete an MD, use the **no** command.

cfm domain *DOMAIN-NAME* **level** *LEVEL*

no cfm domain *DOMAIN-NAME*

Parameters

domain *DOMAIN-NAME*	(Optional) Specifies the MD name as the identifier. It is a string type of maximum length 22. The name does not allow embedded spaces.
level *LEVEL*	Specifies the MD level. The range is from 0 to 7.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to define a maintenance domain and enter the maintenance domain configuration mode. Each maintenance domain has unique name amongst all those used or available to a service provider or operator. It facilitates easy identification of administrative responsibility for each maintenance domain. A unique maintenance level (from 0 to 7) is assigned to define the hierarchical relationship between domains. The larger range of domain has the higher value of level.

If the input is error or the maintenance domain name already exists, it will not create maintenance domain. When the maintenance domain is deleted, the configuration based on it is also deleted.

Example

This example shows how to define the maintenance domain called “op-domain” with maintenance domain level of 2.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)#
```

14-6 cfm global enable

This command is used to enable the CFM function globally. To disable the CFM function globally, use the **no** command.

cfm global enable

no cfm global enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable the CFM globally.

Example

This example shows how to enable CFM globally.

```
Switch# configure terminal
Switch(config)# cfm global enable
Switch(config)#
```

14-7 cfm enable

This command is used to enable the CFM function on the specified physical interface. To disable the CFM function on the specified physical interface, use the **no** command.

cfm enable

no cfm enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable the CFM function on the specified physical interface.

Example

This example shows how to enable the CFM function on the specified physical interface.

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

14-8 cfm lck start

This command is used to start the CFM management lock action. To stop the CFM management lock action, use the **cfm lck stop** command.

cfm lck start mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

cfm lck stop mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Parameters

mepid *MEP-ID*	Specifies the MEP ID.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to start or stop the CFM management lock. This command will result in the MEP to send LCK PDUs to a client level MEP. Verify the status of the CFM management lock action by entering the **show cfm mep** command. The LCK Action item in the **show cfm mep** command will indicate the status of the CFM management lock action is start or stop.

Example

This example shows how to start the management lock.

```
Switch# cfm lck start mepid 1 ma name op-ma domain op-domain
Switch#
```

14-9 cfm linktrace

This command is used to issue a link trace message.

cfm linktrace *MAC-ADDR* **mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[ttl** *TTL***]** **[pdu-priority** *COS-VALUE***]**

Parameters

MAC-ADDR	Specifies the destination MAC address.
mep *MEP-ID*	Specifies the MEP ID to initiate the link-trace function.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.
ttl *TTL*	Specifies the link-trace message's TTL value. The range is from 2 to 255. The default value is 64.
pdu-priority *COS-VALUE*	Specifies the 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as the CCMs and LTMs sent by the MA.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to issue a CFM link trace message.

Example

This example shows how to transmit an LTM to the destination MAC address 00-01-02-03-04-05.

```
Switch# cfm linktrace 00-01-02-03-04-05 mepid 1 ma name op-ma1 domain op-domain1

Transaction ID： 26
```

```
Switch#
```

14-10 cfm loopback test

This command is used to start a CFM loopback test.

cfm loopback test {*MAC-ADDR* **| remote-mepid** *REMOTE-MEPID***} mepid** *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[num** *NUMBER***] [length** *LENGTH* **| pattern** *STRING***] [pdu-priority** *COS-VALUE***]**

Parameters

MAC-ADDR	Specifies the destination MAC address.
remote-mepid *REMOTE-MEPID*	Specifies the destination MEP ID.
mep *MEP-ID*	Specifies the MEPID to initiate the loopback function.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.
num *NUMBER*	Specifies the number of LBMs to be sent. If not specified, the default value is 4.
length *LENGTH*	Specifies the payload length of the LBM to be sent. The range is from 0 to1500. The default is 0.
pattern *STRING*	Specifies an arbitrary amount of data to be included in a Data TLV, along with an indication whether the Data TLV is to be included. It is a string type with maximum 1500. No space can be embedded.
pdu-priority *COS-VALUE*	Specifies the 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as the CCMs and LTMs sent by the MA.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

The user can press CTRL+C to exit the loopback test. The MAC address represents the destination MEP or MIP that can be reached by this MAC address. The MEP represents the source MEP used to initiate the loopback message.

Example

This example shows how to transmit an LBM to the destination MAC address 00-01-02-03-04-05.

```
Switch# cfm loopback test 00-01-02-03-04-05 mepid 1 ma name op-ma1 domain op-domain1

Request timed out.
```

```
Request timed out.
Request timed out.
Request timed out.
CFM loopback statistics for 00-01-02-03-04-05:
Packets: Sent=4, Received=0, Lost=4(100% loss).

Switch# cfm loopback test remote-mepid 2 mepid 1 ma name op-ma1 domain op-domain1

Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
Reply from 00-01-02-03-04-05: bytes=0 time=10ms
CFM loopback statistics for 00-01-02-03-04-05:
    Packets: Sent=4, Received=4, Lost=0(0% loss).

Switch#
```

14-11 cfm ma

This command is used to define a maintenance association and enter the CFM MA Configuration Mode. To delete a maintenance association, use the **no** command.

cfm ma name *MA-NAME* **[vlan** *VLAN-ID***]**

no cfm ma name *MA-NAME*

Parameters

name *MA-NAME*	Specifies the MA with a name as the identifier.
vlan *VLAN-ID*	Specifies the primary VLAN ID of the maintenance association except that the maintenance association is identified by primary VLAN ID.

Default

None.

Command Mode

CFM MD Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to define or delete a maintenance association and enter the CFM MA Configuration Mode. Each maintenance association in a maintenance domain must have a unique maintenance association name. The maintenance associations configured in different maintenance domains may have the same maintenance association identifier. When the maintenance association is deleted, the configuration based on it is also deleted.

Example

This example shows how to create a maintenance association called “op1” which is assigned to the maintenance domain named op-domain.

```
Switch# configure terminal
```

```
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op1 vlan 2
Switch(config-cfm-ma)#
```

14-12 cfm mep

This command is used to define a maintenance association end-point and enter the CFM MEP Configuration Mode. To delete an MEP, use the **no** command.

cfm mep mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[direction {up | down}]**

no cfm mep mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Parameters

mepid *MEP-ID*	Specifies the MEP ID. The range is from 1 to 8191.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.
direction	(Optional) Specifies the direction of the MEP. **Up:** Inward facing (up) MEP. **Down:** Outward facing MEP When creating an MEP, the direction of the MEP should be specified. If not specified, it means to enter the CFM MEP Configuration Mode for an existed MEP.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to define a maintenance association end point. Each MEP configured in the same MA must have a unique MEP ID. The MEP on different MA can have the same MEPID. Before creating a MEP, its MEP ID should be configured in the MA's MEP ID list.

Example

This example shows how to configure an MEP by MPs on the specified physical interface. Assign the direction of the MEP up.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op1 vlan 2
Switch(config-cfm-ma)# mepid-list add 1-2
Switch(config-cfm-ma)# exit
Switch(config-cfm-md)# exit
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain direction up
```

```
Switch(config-cfm-mep)#
```

14-13 clear cfm counter ccm

This command is used to clear CCM counters of all MEPs.

clear cfm counter ccm

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to clear the CCM packet counters of MEPs.

Example

This example shows how to clear the CCM packet counters of all MEPs.

```
Switch# clear cfm counter ccm
Switch#
```

14-14 clear cfm linktrace

This command is used to delete received link trace responses.

clear cfm linktrace {mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **| all}**

Parameters

all	Specifies to clear all link-trace buffers.
mepid *MEP-ID*	Specifies the MEP ID.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to delete the stored link-trace response data that has been initiated by the specified MEP.

Example

This example shows how to delete received link-trace responses.

```
Switch# clear cfm linktrace mepid 1 ma name op-ma1 domain op-domain1
Switch#
```

14-15 clear cfm pkt-cnt interface

This command is used to clear the CFM packet's RX/TX counters of the specified physical interface.

clear cfm pkt-cnt interface {*INTERFACE-ID* **[, | -] | all} [rx] [tx]**

Parameters

INTERFACE-ID	Specifies the interface ID to clear. The allowed interfaces only include physical interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.
rx	(Optional) Specifies the RX counters of the specified physical interface.
tx	(Optional) Specifies the TX counters of the specified physical interface.
all	Specifies to clear all interface's CFM counters.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to clear the physical interface's packet counters. If only the physical interface is specified, it will clear both the RX and TX packet counters of the specified physical interface. If both the physical interface and the RX/TX type is specified, it will clear the RX or TX packet counters of the specified physical interface.

Example

This example shows how to clear TX packet counters of eth 1/0/1.

```
Switch# clear cfm pkt-cnt interface eth1/0/1 tx
```

```
Switch#
```

14-16 fault-alarm

This command is used to control the types of fault alarms sent by the MEP. To reset to the default setting, use **no** command.

fault-alarm {none | all | mac-status | remote-ccm | error-ccm | xcon-ccm}

no fault-alarm

Parameters

none	Specifies that no fault alarm will be sent.
all	Specifies that all types of fault alarms will be sent.
mac-status	Specifies that only the fault alarms whose priority is equal to or higher than “Some Remote MEP MAC Status Errors” will be sent.
remote-ccm	Specifies that only the fault alarms whose priority is equal to or higher than “Some Remote MEPs Down” will be sent.
error-ccm	Specifies that only the fault alarms whose priority is equal to or higher than “Error CCM Received” will be sent.
xcon-ccm	Specifies that only the fault alarms whose priority is equal to or higher than “Cross-connect CCM Received” will be sent.

Default

By default, this option is **none**.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to control the types of fault alarms sent by the MEP.

Example

This example shows how to configure the MEP to send all types of fault alarms.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# fault-alarm all
Switch(config-cfm-mep)#
```

14-17 lck

This command is used to configure the parameters of the LCK function. To disable the CFM LCK function, use the **no** command.

lck [period *PERIOD***] [level** *LEVEL***]**

no lck [period | level]

Parameters

period *PERIOD*	(Optional) Specifies the transmitting interval of the LCK PDU. It can be 1sec or 1min.The default period is 1 second.
level *LEVEL*	(Optional) Specifies the client level ID to which the MEP sends the LCK PDU. The default client maintenance domain level is the maintenance domain level that the most immediate client layer MIPs and MEPs exist on. The range is from 0 to 7.

Default

By default, this option is disabled.

The default period is 1 second.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the parameters of the LCK function on a MEP. If only the MEP name is defined, it will enable the CFM LCK function. This default client maintenance domain level is not a fixed value. It may change when creating or deleting higher level maintenance domain and MA on the device.

When the most immediate client layer MIPs and MEPs do not exist, the default client maintenance domain level cannot be calculated. If the default client maintenance domain level cannot be calculated and the user does not designate a client level, the LCK PDU cannot be transmitted.

Example

This example shows how to configure the LCK function so that it has a client level of 5.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# lck level 5
```

14-18 mepid-list

This command is used to create an MEP ID list.

mepid-list {add | delete} *MEPID-LIST*

Parameters

mepid-list *MEPID-LIST*	Specifies the MEP IDs contained in the MA. The range of the MEPID is from 1 to 8191.

Default

None.

Command Mode

CFM MA Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an MEP ID list in a maintenance association. To add an MEP ID into the list, use the **cfm mepid-list add** command. To delete an MEP ID from the list, use the **cfm mepid-list delete** command. Before defining an MEP, the MEP ID list must be created and the MEP's ID must be added into the list.

Example

This example shows how to create an MEP ID list and add the MEP IDs 1 and 2 into it for a maintenance association.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op1 vlan 2
Switch(config-cfm-ma)# mepid-list add 1,2
Switch(config-cfm-ma)#
```

14-19 mip creation (cfm md configuration)

This command is used to configure the default MIP creation in a maintenance domain. To reset the configuration of the MIP creation to the default setting, use **no** command.

mip creation {none | auto | explicit}

no mip creation

Parameters

none	Specifies not to create the MIP for a maintenance domain.
auto	Specifies that MIPs will always be created on any port in this maintenance domain, if that port is not configured as an MEP of this maintenance domain. For an intermediate switch in an MA, the setting must be automatically in order for the MIPs to be created on this device.
explicit	Specifies that MIPs can be created on ports that has an existing lower level MEP configured on it and that the port is not configured as an MEP of this maintenance domain.

Default

By default, this option is **none**.

Command Mode

CFM MD Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the default MIP creation for a maintenance domain.

The creation of MIPs on a maintenance domain is useful for tracing the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP. An enumerated value indicates whether the management entity can create MIP Half Functions (MHF) for a maintenance domain.

This command setting acts as the default setting for MA contained by this MD to automatically create MIPs. Use the **mip creation** command in the CFM MA Configuration Mode not to follow this default setting.

Example

This example shows how to configure the MIP creation to “auto”.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# mip creation auto
Switch(config-cfm-md)#
```

14-20 mip creation (cfm ma configuration)

This command is used to configure the MIP creation for an MA. To reset the configuration of the MIP creation to the default setting, use the **no** command.

mip creation {none | auto | explicit | defer}

no mip creation

Parameters

none	Specifies not to create the MIP on ports in an MA.
auto	Specifies that MIPs can always be created on any port in an MA, if that port is not configured with an MEP of this MA. For an intermediate switch in an MA, the setting must be automatic in order for the MIPs to be created on this device.
explicit	Specifies that MIPs can be created on ports which has an existing lower level MEP configured on it, and that port is not configured with an MEP of this MA.
defer	Specifies to inherit the settings configured for the maintenance domain that the MA is associated with. This is the default value.

Default

By default, this option is **defer**.

Command Mode

CFM MA Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the MIP creation for an MA. By default, the setting follows the global mode MIP creation command configuration,

The creation of MIPs on a maintenance association is useful for tracing the link, MIP by MIP. It also allows the user to perform a loopback from an MEP to an MIP. An enumerated value indicates whether the management entity can create MHFs for this maintenance association.

Example

This example shows how to configure a maintenance association MIP creation to “auto”.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op-ma1 vlan 2
Switch(config-cfm-ma)#  mip  creation auto
Switch(config-cfm-ma)#
```

14-21 mep enable

This command is used to enable the MEP state. To disable the MEP state, use the **no** command.

mep enable

no mep enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable and disable MEP state.

Example

This example shows how to enable the MEP state.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# mep enable
Switch(config-cfm-mep)#
```

14-22 pdu-priority

This command is used to define the 802.1p priority that is set in the CCM and the LTM messages transmitted by the MEP. Use the **no** form of the command to reset to the default setting.

pdu-priority *COS-VALUE*

no pdu-priority

Parameters

pdu-priority *COS-VALUE*	Specifies that the 802.1p priority is set in the CCM and the LTM messages transmitted by the MEP. The range of the value is from 0 to 7.

Default

By default, the PDU priority is level 7.

Command Mode

CFM MEP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to define the 802.1p priority that is set in the CCM and the LTM messages transmitted by the MEP.

Example

This example shows how to define the 802.1p priority that is set in the CCM and the LTM messages transmitted by the MEP.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# cfm mep mepid 1 ma name op1 domain op-domain
Switch(config-cfm-mep)# pdu-priority 2
Switch(config-cfm-mep)#
```

14-23 sender-id (cfm md configuration)

This command is used to configure the default transmission of the sender ID TLV by MPs in a maintenance domain. To reset the configuration of the transmission of the sender ID TLV to the default setting, use the **no** command.

sender-id {none | chassis | manage | chassis-manage}

no sender-id

Parameters

none	Specifies not to transmit the sender ID TLV.
chassis	Specifies to transmit the sender ID TLV with the chassis ID information.
manage	Specifies to transmit the sender ID TLV with the managed address information.
chassis-manage	Specifies to transmit the sender ID TLV with the chassis ID information and the managed address information.

Default

None.

Command Mode

CFM MD Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the default transmission of the sender ID TLV by MPs contained by the MD. An enumerated value indicates what, if anything, is to be included in the sender ID TLV transmitted by MPs configured in this maintenance domain.

Example

This example shows how to configure sender ID TLV by MPs. Transmit the sender ID TLV with the chassis ID information.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# sender-id chassis
Switch(config-cfm-md)#
```

14-24 sender-id (cfm ma configuration)

This command is used to configure the transmission of the sender ID TLV by MPs for an MA. To reset the configuration of the transmission of the sender ID TLV to default setting, use the **no** command

sender-id {none | chassis | manage | chassis-manage | defer}

no sender-id

Parameters

none	Specifies not to transmit the sender ID TLV. In the CFM hardware mode, the value is fixed to none.
chassis	Specifies to transmit the sender ID TLV with the chassis ID information.
manage	Specifies to transmit the sender ID TLV with the managed address information.
chassis-manage	Specifies to transmit the sender ID TLV with the chassis ID information and the managed address information.
defer	Specifies to inherit the setting configured for the maintenance domain that the MA is associated with. This is the default value.

Default

By default, this option is **defer**.

Command Mode

CFM MA Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the transmission of the sender ID TLV by MPs for an MA. An enumerated value indicates what, if anything, is to be included in the sender ID TLV transmitted by MPs configured in this maintenance association.

Example

This example shows how to configure the sender ID TLV by MPs on the CFM MA Configuration Mode. Transmit the sender ID TLV with the chassis ID information.

```
Switch# configure terminal
Switch(config)# cfm domain op-domain level 2
Switch(config-cfm-md)# cfm ma name op-ma1 vlan 2
Switch(config-cfm-ma)# sender-id chassis
Switch(config-cfm-ma)#
```

14-25 show cfm

This command is used to display the CFM global state.

show cfm

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the CFM global state.

Example

This example shows how to display the CFM global state.

```
Switch# show cfm

       CFM State: Enabled
       Domain Name: md5   Level: 5
       Domain Name: md6   Level: 2

Switch#
```

14-26 show cfm counter ccm

This command is used to display the CFM CCM counters of all MEPs.

show cfm counter ccm

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is used to display the CCM RX packet counters of all MEPs.

Example

This example shows how to display CCM packet counters of all MEPs

```
Switch# show cfm counter ccm

CCM counters:
MEPID: 1   VID: 1    Level: 2    Direction: up     Port: eth1/0/1
       XCON: 9            Error: 8    Normal: 100
MEPID: 2   VID: 1    Level: 2    Direction: up     Port: eth1/0/11
       XCON: 9            Error: 8    Normal: 100

Total:
     XCON: 18   Error: 16   Normal: 200

Switch#
```

Display Parameters

XCON	It indicates that one or more cross connect CCMs has been received.
Error	It indicates that one or more invalid CCMs have been received.
Normal	It indicates that one or more normal CCMs have been received.

14-27 show cfm domain

This command is used to display the CFM maintenance domain information.

show cfm domain *DOMAIN-NAME*

Parameters

DOMAIN-NAME	Specifies the maintenance domain name as the identifier. It is a string type of maximum length 22. If not specified, all domains are displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display CFM maintenance domain information.

Example

This example shows how to display CFM maintenance domain information.

```
Switch# show cfm domain md5

    Domain Name: md5
    Domain Level: 5
    MIP Creation: Auto
    SenderID TLV: Chassis
    MA Name: ma5

Switch#
```

14-28 show cfm interface

This command is used to display the CFM state on the specified physical interface.

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

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface ID to display. The allowed interfaces only include physical interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the CFM state on the specified physical ports.

Example

This example shows how to display the CFM state on the specified physical ports.

```
Switch# show cfm interface eth1/0/12

eth1/0/12
CFM is enabled
MAC Address   : 00-09-5A-B9-AC-1B

Domain Name: md5
Level: 5
MA Name: ma5
 VID: 10
    MEPID: 2
 Direction：down

Domain Name: md6
Level: 6
MA Name: ma6
VID: 10
MEPID: MIP

Switch#
```

14-29 show cfm linktrace

This command is used to display the link trace responses.

show cfm linktrace [mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[trans-id** *ID***]]**

Parameters

mepid *MEP-ID*	Specifies the MEP ID.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.
trans-id *ID*	Specifies the identifier of the transaction to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the link-trace responses. The maximum link-trace responses a device can hold is 64.

Example

This example shows how to display the link-trace responses.

```
Switch# show cfm linktrace mepid 1 ma name op-ma domain op-domain trans-id 0

Transaction ID: 0
From MEPID 1 to 00-07-00-00-00-1C
Start Time: 2013-11-02 11:35:11
Hop: 1
       MEPID: -
       Ingress MAC Address: 00-00-00-00-00-00
       Egress MAC Address: 00-09-5A-B9-AC-1B
       Forwarded: Yes            Relay Action: FDB

Hop: 2
       MEPID: 2
       Ingress MAC Address: 00-07-00-00-00-1C
       Egress MAC Address: 00-00-00-00-00-00
       Forwarded: No             Relay Action: Hit

Switch#
```

Display Parameters

Relay Action	**Hit:** The LTM reached an MP whose MAC address matches the target MAC address. **FDB:** The Egress Port was determined by consulting the Filtering Database. **MPDB:** The Egress Port was determined by consulting the MIP CCM Database.

14-30 show cfm ma

This command is used to display the CFM maintenance association information.

show cfm ma name *MA-NAME* **domain** *DOMAIN-NAME*

Parameters

domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.
name *MA-NAME*	Specifies the MA name as the identifier.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the CFM maintenance association information.

Example

This example shows how to display CFM maintenance association information.

```
Switch# show cfm ma name ma5 domain md5

      MA Name: ma5
      MA VID: 10
      MIP Creation: Auto
      CCM Interval: 10 seconds
      SenderID TLV: Chassis
      MEPID List: 1-2
            MEPID: 1    Port：eth1/0/2    Direction: up

Switch#
```

Display Parameters

MEPID	The MEP already created in the MA.
Port	The MEP port.
Direction	The MEP direction (up or down).

14-31 show cfm mep

This command is used to display the MEPs that have configurations.

show cfm mepid *MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME*

Parameters

mepid *MEP-ID*	Specifies the MEP ID. The range is from 1 to 8191.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the MEPs that have configurations.

Example

This example shows how to display the MEPs that have configurations.

```
Switch# show cfm mepid 1 ma name op-ma domain op-domain

MEPID: 2
      Port: eth1/0/9
      Direction: Up
      CFM Port Status: Enabled
      MAC Address: 00-09-5A-B9-AC-18
      MEP State: Enabled
      CCM State: Enabled
      PDU Priority: 7
      Fault Alarm: Disabled
      Alarm Time: 250 centiseconds
      Alarm Reset Time: 1000 centiseconds
      Highest Fault: Some Remote MEP Down
      AIS State: Disabled
      AIS Period: 1 Second
      AIS Client Level: Invalid
      AIS Status: Not Detected
      LCK State: Disabled
      LCK Period: 1 Second
      LCK Client Level: Invalid
      LCK Status: Not Detected
      LCK Action：Stop
      Out-of-Sequence CCMs Received: 0
      Cross-connect CCMs Received: 0
      Error CCMs Received: 0   Normal CCMs   Received: 0
      Port Status CCMs Received: 0   If Status CCMs Received: 0
      CCMs transmitted: 14813   In-order LBRs Received: 0
      Out-of-order LBRs Received: 0   Next LTM Trans ID: 0
      Unexpected LTRs Received: 0   LBMs Transmitted: 0
      AIS PDUs Received: 0   AIS PDUs Transmitted: 0
      LCK PDUs Received: 0   LCK PDUs Transmitted: 0

Switch#
```

Display Parameters

Highest Fault	**None:** No defect has been present since the last FNG_RESET state. **Some Remote MEP Defect Indication:** The last CCM received by this MEP from some remote MEP indicates that remote MEP detects some defect. **Some Remote MEP MAC Status Error:** The last CCM received by this MEP indicated that the remote MEP's associated MAC is reporting an error status. **Some Remote MEP Down:** This MEP is not receiving CCMs from some other MEP in its configured list. **Error CCM Received:** This MEP is receiving invalid CCMs, which may be caused by configuration error. **Cross-connect CCM Received:** This MEP is receiving CCMs that

	could be from some other MA.
Fault Alarm	**All:** All types of fault alarms will be sent. **Some Remote MEP Defect Indication:** The last CCM received by this MEP from some remote MEP indicates that remote MEP detects some defect. **Some Remote MEP MAC Status Error:** The last CCM received by this MEP indicated that the remote MEP's associated MAC is reporting an error status. **Some Remote MEP Down:** This MEP is not receiving CCMs from some other MEP in its configured list. **Error CCM Received:** This MEP is receiving invalid CCMs, which may be caused by configuration error. **Cross-connect CCM Received:** This MEP is receiving CCMs that could be from some other MA. **Disabled:** The fault alarm function is disabled.

14-32 show cfm mep fault

This command is used to display the MEPs that have faults.

show cfm mep fault

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This display provides an overview of the fault status by the MEPs. This command displays all the fault conditions that were detected by the MEPs contained in the specified MA.

Example

This example shows how to display the MEPs that have faults.

```
Switch# show cfm mep fault

Domain Name: md5
MA Name: ma5
MEPID: 2
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal

Domain Name: md6
```

```
MA Name: ma6
MEPID: 3
Status: Some Remote MEP Down
AIS Status: Normal
LCK Status: Normal

Switch#
```

Display Parameters

Status	**None:** No defect has been present since the last FNG_RESET state. **Some Remote MEP Defect Indication:** The last CCM received by this MEP from some remote MEP indicates that remote MEP detects some defect. **Some Remote MEP MAC Status Error:** The last CCM received by this MEP indicated that the remote MEP's associated MAC is reporting an error status. **Some Remote MEP Down:** This MEP is not receiving CCMs from some other MEP in its configured list. **Error CCM Received:** This MEP is receiving invalid CCMs, which may be caused by configuration error. **Cross-connect CCM Received:** This MEP is receiving CCMs that could be from some other MA.
AIS Status	**AIS received:** Indicates the AIS have been received. **Normal:** Indicates none has been received.
LCK Status	**LCK received:** Indicates the LCK have been received **Normal:** Indicates none has been received.

14-33 show cfm mip ccm

This command is used to display the MIP CCM database entries.

show cfm mip ccm

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the MIP CCM database entries.

Example

This example shows how to display the MIP CCM database entries.

```
Switch# show cfm mip ccm

      VID: 10
      MAC Address: 00-07-00-00-00-1C
      Port: eth1/0/12

      VID: 10
      MAC Address: 00-07-00-00-00-1E
      Port: eth1/0/14

      Total: 2

Switch#
```

14-34 show cfm remote-mep

This command is used to display the remote MEP information.

show cfm remote-mep mepid *LOCAL-MEP-ID* **ma name** *MA-NAME* **domain** *DOMAIN-NAME* **[remote-mepid** *REMOTE-MEPID***]**

Parameters

mepid *MEP-ID*	Specifies the MEP ID.
name *MA-NAME*	Specifies the MA name as the identifier.
domain *DOMAIN-NAME*	Specifies the MD name as the identifier. It is a string type of maximum length 22.
remote-mepid *REMOTE-MEPID*	(Optional) Specifies the remote MEP ID. The range is from 1 to 8191.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the remote MEP information.

Example

This example shows how to display all the remote MEP information seen by local MEP 1.

```
Switch# show cfm remote-mep mepid 1 ma name op-ma domain op-domain

      Remote MEPID: 2
      MAC Address: 00-11-22-33-44-02
      Status: OK   RDI: Yes
```

```
      Port State: Up   Interface Status: No
      Last CCM Serial Number: 1000
      Sender Chassis ID: None
      Sender Management Address: 10.90.90.90:161
      Detect Time: 2013-11-01 17:00:00

      Remote MEPID: 3
      MAC Address: 11-22-33-44-02-05
      Status: OK   RDI: Yes
      Port State: Up   Interface Status: No
      Last CCM Serial Number: 200
      Sender Chassis ID: None
      Sender Management Address: 10.90.90.90:161
      Detect Time: 2013-11-01 17:00:00

Switch#
```

This example shows how to display the remote MEP information.

```
Switch# show cfm remote-mep mepid 1 ma name op-ma domain op-domain remote-mepid 2

      Remote MEPID: 2
      MAC Address: 00-11-22-33-44-02
      Status: OK   RDI: Yes
      Port State: Up   Interface Status: No
      Last CCM Serial Number: 1000
      Sender Chassis ID: None
      Sender Management Address: 10.90.90.90:161
      Detect Time: 2013-11-01 17:00:00

Switch#
```

Display Parameters

Status	**Idle:** The momentary state during reset. **Start:** The timer has not expired since the state machine was reset, and no valid. The CCM has yet been received. **Failed:** The timer has expired, both since the state machine was reset, and since a valid CCM was received. **OK:** The timer has not expired since a valid CCM was received.
RDI	**Yes:** Indicates the state of the RDI bit in the last received CCM. **No:** If none has been received.
Port State	The port state indicates the ability of the bridge port on which the transmitting MEP resides to pass ordinary data, regardless of the status of the MAC. **None:** Indicates either that no CCM has been received or that no port status TLV was present in the last CCM received. **Blocked:** Ordinary data cannot pass freely through the port on which the remote MEP resides. **Up:** Ordinary data can pass freely through the port on which the remote MEP resides.
Interface Status	**None:** Indicates either that no CCM has been received or that no

	interface status TLV was present in the last CCM received. **Up:** The interface is ready to pass packets. **Down:** The interface cannot pass packets. **Testing:** The interface is in some test mode. **Unknown:** The interface status cannot be determined for some reason. **Dormant:** The interface is not in a state to pass packets but is in a pending state, waiting for some external event. **Notpresent:** Some component of the interface is missing. **Lowerlayerdown:** The interface is down due to state of the lower layer interfaces.

14-35 show cfm pkt-cnt interface

This command is used to display the CFM packet's RX/TX counters of the specified physical interface.

show cfm pkt-cnt interface [*INTERFACE-ID* **[, | -]] [rx] [tx]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID to display. The allowed interfaces only include physical interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.
rx	(Optional) Specifies the RX counters of the specified physical interface.
tx	(Optional) Specifies the TX counters of the specified physical interface.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is used to display physical interface's packet counters. If interfaces are not specified, then counters for all interfaces are displayed. If only the physical interface is specified, it will display both the RX and TX packet counters of the specified physical interface. If the RX/TX type is specified, it will display the RX or TX packet counters of all physical interfaces.

Example

This example shows how to display packet counters of eth 1/0/1.

```
Switch# show cfm pkt-cnt interface eth1/0/1
```

```
eth1/0/1
      CFM RX Statistics
            AllPkt: 0            CCM: 0
            LBR: 0               LBM: 0
            LTR: 0               LTM: 0
            VidDrop: 0           OpcoDrop: 0
      CFM TX Statistics
            AllPkt: 0            CCM: 0
            LBR: 0               LBM: 0
            LTR: 0               LTM: 0

Switch#
```

This example shows how to display RX packet counters of eth 1/0/1.

```
Switch# show cfm pkt-cnt interface eth1/0/1 rx

eth1/0/1
        CFM RX Statistics
                AllPkt: 0               CCM: 0
                LBR: 0                  LBM: 0
                LTR: 0                  LTM: 0
                VidDrop: 0              OpcoDrop: 0

Switch#
```

This example shows how to display TX packet counters of eth 1/0/1.

```
Switch# show cfm pkt-cnt interface eth1/0/1 tx

eth1/0/1
        CFM TX Statistics
                AllPkt: 0               CCM: 0
                LBR: 0                  LBM: 0
                LTR: 0                  LTM: 0

Switch#
```

Display Parameters

VidDrop	It indicates that the packets are dropped out of the VLAN.
OpcoDrop	It indicates that the packets are dropped when cannot match the normal op-code.

14-36 cfm mp-ltr-all

This command is used to enable the function where all MPs reply to LTRs. To disable this function, use the **no** command.

cfm mp-ltr-all

no cfm mp-ltr-all

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

According to IEEE 802.1ag, a Bridge replies with one LTR to an LTM. This command can make all MPs on an LTM's forwarding path reply with LTRs, whether they are on a Bridge or not.

Example

This example shows how to enable this function.

```
Switch# configure terminal
Switch(config)# cfm mp-ltr-all
Switch(config)#
```

15. CPU Access Control List (ACL) Commands

15-1 soft-acl filter-map

This command is used to create or modify a software ACL filter map. This command will enter into the software ACL filter map configuration mode. Use the **no** command to remove a software ACL filter map.

soft-acl filter-map *NAME*

no soft-acl filter-map *NAME*

Parameters

NAME	Specifies the name of the software ACL filter map to be configured. The name can be up to 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter into the software ACL filter map configuration mode, to associate some pre-defined ACL access list(s) to filter packets received at CPU. Multiple software ACL filter maps can be configured.

Example

This example shows how to create a software ACL filter map named “cpu_filter”.

```
Switch# configure terminal
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)#
```

15-2 match access-group

This command is used to associate an access list to the software ACL filter map. Use the **no** command to remove an association.

SEQUENCE-NUMBER **match mac access-group** *NAME*

SEQUENCE-NUMBER **match ip access-group** *NAME*

SEQUENCE-NUMBER **match ipv6 access-group** *NAME*

SEQUENCE-NUMBER **match expert access-group** *NAME*

no match {mac | ip | ipv6 | expert} access-group

Parameters

SEQUENCE-NUMBER	Specifies the sequence number of the associated match entry. The range is from 1 to 65535. The lower the number is, the higher the priority of the access list.
NAME	Specifies the ACL access list name to be match.

Default

None.

Command Mode

Software ACL Filter Map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to associate an access list to a software ACL filter map. Multiple access lists can be associated within a software ACL filter map. However, they should be different types (expert, MAC, IP, and IPv6). When the same type access list is associated, each succeeding command overwrites the previous command.

Sequence numbers determines the processing priority of an associated access list in a filter map. The access list with a smaller sequence number takes higher precedence. If the associated access list with same sequence number exists, they are processed in the following order: expert access list, MAC access list, IP access list, IPv6 access list.

Example

This example shows how to attach an IP access list named “cpu-acl” and MAC access list named mac4001 to the software ACL filter map “cpu_filter”.

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)#
```

15-3 match interface

This command is used to configure matching ingress interface(s). Use the **no** form command to remove the matching ingress interface(s).

match interface *INTERFACE-ID* **[, | -]**

no match interface {all | *INTERFACE-ID* **[, | -]}**

Parameters

INTERFACE-ID	Specifies the matching interface ID. Valid interfaces are physical

	interfaces.
,	(Optional) Specifies a series of physical interfaces. No space before and after the comma.
-	(Optional) Specifies a series of physical interfaces. No space before and after the comma.
all	Specifies that in the **no** form of this command, to remove all matching ingress interface(s).

Default

None.

Command Mode

Software ACL Filter Map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A software ACL filter map will be activated when there is one or more matching interface(s) are configured. In other words, if no matching interface is configured, this filter map won't take effect.

When a packet is received at CPU and the ingress interface is configured in a software ACL filter map, the switch will look up the associated access list(s) of the corresponding filter map.

The associated access list with the highest priority in the filter map will be checked at first. Once match is found, the other ACL access list(s) will be ignored. Otherwise, the access list with the next highest priority will be looked up and so on.

Within an access list, the similar checking sequence is used. The rule with a smaller sequence number takes higher precedence. Once match is found, others will be ignored.

Finally, if no match is found, the packet will be permitted, and it can be continually processed by other functions.

If the matching action is 'permit', it will be passed to other functions. Else if the action is 'drop', the packet will be dropped.

In other words, the action of software ACL is based on the explicitly configured permit/deny entry. A packet is permitted if it does not match any explicit permit or deny rule.

An interface can belong to at most one filter map. When an interface is configured to a new filter map, the interface will be removed from the previous filter map.

Example

This example shows how to configure a matching interface, eth1/0/1, to the software ACL filter map, "cpu_filter".

```
Switch# configure terminal
Switch(config)# ip access-list cpu-acl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# mac access-list extended mac4001
Switch(config-mac-ext-acl)# 25 deny host 0013.0049.8272 any
Switch(config-mac-ext-acl)# exit
Switch(config)# soft-acl filter-map cpu_filter
Switch(config-soft-acl)# 2 match ip access-group cpu-acl
Switch(config-soft-acl)# 3 match mac access-group mac4001
Switch(config-soft-acl)# match interface eth1/0/1
Switch(config-soft-acl)#
```

15-4 show soft-acl

This command is used to display the information of software ACL filter maps.

show soft-acl filter-map [*NAME***]**

Parameters

NAME	(Optional) Specifies the name of the software ACL filter map to be displayed.

Default

None.

Command Mode

Any Configured Mode.

Command Default Level

Level: 1.

Usage Guideline

Use the command to display the specified software ACL filter map. If no name is specified, all software ACL filter maps will be displayed.

Example

This example shows how to display the software ACL filter map.

```
Switch# show soft-acl filter-map

 Software ACL Filter Map
   cpu_filter:
 Match Access-list(s):
   IP(2): Ext-ip
   MAC(3):mac4001
 Match Ingress Interface(s):
   eth1/0/1

Switch#
```

Display Parameters

IP(N)	The access list type. The number in parenthesis means the sequence number of the associated access list.

16. CPU Port Statistics Commands

16-1 debug show cpu port

This command is used to display statistics for Layer 2 or Layer 3 control packets that are trapped to the CPU.

debug show cpu port [l2 | l3 [unicast | multicast] | protocol *NAME***]**

Parameters

l2	(Optional) Specifies to display statistic counters of Layer 2 control packets.
l3	(Optional) Specifies to display statistic counters of Layer 3 control packets.
unicast	Specifies to display statistic counters of Layer 3 unicast routing and Layer 3 application control packets.
multicast	Specifies to display statistic counters of Layer 3 multicast routing control packets.
protocol *NAME*	(Optional) Specifies the name of protocol. It is case sensitive.

Default

None.

Command Mode

Privileged EXEC Mode or Any Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is use to display statistics for Layer 2 and Layer 3 control packets that are trapped to the CPU.

Example

This example shows how to display all Layer 2 and Layer 3 protocol control packets that are trapped to the CPU.

```
Switch# debug show cpu port

Type                             PPS        Total       Drop
-------------------------------  ---------  ----------  -----------
OSPFv2                           0          0           0
OSPFv3                           0          0           0
RIP                              0          0           0
RIPng                            0          0           0
LACP                             0          0           0
802.1X                           0          0           0
Stacking                         0          810         0
GVRP                             0          0           0
STP                              0          0           0
CFM                              0          0           0
```

```
LLDP                            0           0           0
CTP                             0           0           0
BGP                             0           0           0
DHCP                            0           0           0
DHCPv6                          0           0           0
ERPS                            0           0           0
OAM                             0           0           0
IGMP                            0           0           0
MLD                             0           0           0
PIM-IPv4                        0           0           0
PIM-IPv6                        0           0           0
DVMRP                           0           0           0
Reserved-IPv4-IPMC              0           0           0
Reserved-IPv6-IPMC              0           0           0
Unknown-IPv4-IPMC               0           0           0
Unknown-IPv6-IPMC               0           0           0
ARP                             0           39          34
ICMP                            0           0           0
NDP                             0           0           0
ICMPv6                          0           0           0
SNTP                            0           0           0
DNS                             0           0           0
TFTP                            0           0           0
RCP                             0           0           0
SMTP                            0           0           0
Telnet                          0           0           0
UDP-Helper                      0           0           0
VRRP                            0           0           0

Switch#
```

16-2 debug clear cpu port

This command is used to reset all counters for Layer 2 or Layer 3 control packets that are trapped to the CPU.

debug clear cpu port

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to reset all counters for Layer 2 or Layer 3 control packets that are trapped to the CPU.

Example

This example shows how to clear all statistics counters.

```
Switch# debug clear cpu port
Switch#
```

17. Debug Commands

17-1 debug enable

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

debug enable

no debug enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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

17-2 debug output

This command is used to specify the output for the debug messages of individual modules.

debug output {module <*MODULE-LIST*> | all} {buffer | console}

no debug output {module <*MODULE-LIST*> | all}

Parameters

<*MODULE-LIST*>	Specifies the module list to output the debug messages. Leave a space between modules.
all	Specifies to output the debug messages of all modules to the specified destination.
buffer	Specifies to output the debug message to the debug buffer.
console	Specifies to output the debug messages to the local console.

Default

The default debug output is buffer.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to set a specified module's debug message output to debug to the buffer or the local console. Use the **show debug output** command to display the module's string information. By default, module debug message is output to the debug buffer. The module debug message will be output when the module owned debug setting is enabled and the global mode debug enable command is enabled.

Example

This example shows how to configure all the module's debug messages to output to the debug buffer.

```
Switch# debug output all buffer
Switch#
```

17-3 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.

Command Default Level

Level: 15.

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

17-4 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* **| ftp:** *//USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL* **| rcp:** *//USER-NAME@LOCATION/DESTINATION-URL***} [vrf** *VRF-NAME***]**

Parameters

SOURCE-URL	Specifies the source URL for the source file to be copied. It must be one of the following keywords. **buffer:** Specifies to copy the debug buffer information. **error-log:** Specifies to copy the error log information. **tech-support:** Specifies to copy the technical support information.
LOCATION	Specifies the IPv4 or IPv6 address of the TFTP/FTP/RCP server.
USER-NAME	Specifies the user name on the FTP/RCP server.
PASSWORD	Specifies the password for the user.
VRF-NAME	Specifies the name of the VRF instance which the TFTP/FTP/RCP server belongs to.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

None.

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#
```

17-5 debug clear buffer

This command is used to clear the debug buffer.

debug clear buffer

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to clear the debug buffer information.

Example

This example shows how to clear the debug buffer information.

```
Switch# debug clear buffer
Switch#
```

17-6 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.

Command Default Level

Level: 15.

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#
```

17-7 debug show buffer

This command is used to display the content of the debug buffer or utilization information of the debug buffer.

debug show buffer [utilization]

Parameters

utilization	(Optional) Specifies to display the utilization of the debug buffer. If not specified, this will display the content in the buffer.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the content of the debug buffer or utilization information of the debug buffer.

Example

This example shows how to display the debug buffer information.

```
Switch# debug show buffer

Debug buffer is empty

Switch#
```

This example shows how to display the debug buffer utilization.

```
Switch# debug show buffer utilization

Debug buffer is allocated from system memory
Total size is 2M
Utilization is 30%

Switch#
```

17-8 debug show output

This command is used to display the debug status and output information of the modules.

debug show output

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the information about the debug status and message output of the modules.

Example

This example shows how to display the debug message output information of the modules.

```
Switch# debug show output

Debug Global State  : Disabled

Module name           Output    Enabled
----------------      --------  -------------------------------------
DHCPv6_CLIENT         buffer    No
DHCPv6_RELAY          buffer    No
OSPFV2                buffer    No
BGP                   buffer    No
VRRP                  buffer    No
RIPNG                 buffer    No

Switch#
```

17-9 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.

Command Default Level

Level: 15.

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

                                  <Output truncated>
```

17-10 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.

Command Default Level

Level: 15.

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-3600 Gigabit Ethernet Switch
#                         Technical Support Information
#
#                           Firmware: Build 2.00.012
#          Copyright(C) 2013  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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

[SYS 2013-9-8 08:59:20]

Boot Time     : 8 Sep 2013  08:54:00
RTC Time      : 2013/09/08 08:59:20
Boot PROM Version    : Build 1.10.008
Firmware Version     : Build 2.00.012
Hardware Version     :
MAC Address   : 00-01-02-03-04-05
MAC Address Number   : 0A2G           □□□□□□□□□□

********************   System Log   ********************

[SYS_LOG 2013-9-8 08:59:20]

Index  Date   Time   Level  Log Text
-----  ----------    --------      -------      ---------------------------------------
-------

4      2013-09-08    08:54:58      INFO(6)      Successful login through Console
(Username:
                           Anonymous)
3      2013-09-08    08:54:32      INFO(6)      Port 4 link up, 100Mbps FULL duplex
2      2013-09-08    08:54:27      CRIT(2)      System started up
1      2013-09-08    08:54:27      INFO(6)      MSTP(8):Spanning Tree MST configuration
ID
                           name and revision level change (name:00:01:02:
                           03:04:05 revision level:0)

********************   Layer One Information   ********************
```

```
[PORT 2013-9-8 09:18:22]

[MIRROR 2013-9-8 09:18:22]


 ****************** Mirror ******************
Mirror SW table:
      State: Disable


********************   Layer Two Information   ********************

[VLAN 2013-9-8 09:18:22]

********************************************************************************

[LBD 2013-9-8 10:56:47]

 LBD is disable

[TRAFFIC_SEG 2013-9-8 10:56:47]
......

                                  <Output truncated>
```

17-11 debug show cpu utilization

This command is used to display the total CPU utilization and the CPU utilization per process.

debug show cpu utilization

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the information about CPU and task utilization

Example

This example shows how to display the CPU utilization per process information.

```
Switch# debug show cpu utilization
```

```
Five seconds -   8 %         One minute -   8 %         Five minutes -  13 %

Process Name         5Sec     1Min     5Min
-----------------   ------   ------   ------
OS_UTIL              96 %     93 %     81 %
SYS_Ctr               9 %      2 %      2 %
FAN_Pooling           4 %      3 %      2 %
bcmRX                 3 %      3 %      3 %
bcmL2X.0              2 %      2 %      2 %
bcmCNTR.0             2 %      2 %      2 %
ST_PERI               2 %      1 %      1 %
ST_RxPkt              1 %      1 %      1 %
HISR1                 1 %      1 %      1 %

Switch#
```

18. DHCP Auto-Configuration Commands

18-1 autoconfig enable

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

Command Default Level

Level: 15.

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 how to enable auto-configuration.

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

18-2 show autoconfig

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

show autoconfig

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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#
```

19. DHCP Client Commands

19-1 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 the setting to the default.

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

no ip dhcp client class-id

Parameters

STRING	Specifies the vendor class identifier in the string form. The maximum length of the string is 32.
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.

Command Default Level

Level: 12.

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. Option 60 will not be sent with discover messages unless the class identifier is configured for the interface.

Example

This example shows how to enable the DHCP client, enable the sending of the Vendor Class Identifier, and specifies its value as VOIP-Device for VLAN 100.

```
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)#
```

19-2 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.

Command Default Level

Level: 12.

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)#
```

19-3 ip dhcp client hostname

This command is used to specify the value of the host name option to be sent with the DHCP discover message. Use the **no** form of this command to revert the setting to the default

ip dhcp client hostname *HOST-NAME*

no ip dhcp client hostname

Parameters

HOST-NAME	Specifies the host name. The maximum length is 64 characters. The host name must start with a letter, end with a letter or digit, and only with interior characters letters, digits, and hyphens.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the host name string (Option 12) to be sent with the DHCP 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. If this option is not configured, the switch will be sent messages with no Option 12 configured.

Example

This example shows how to set the host name option value to Site-A-Switch.

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

19-4 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.

Command Default Level

Level: 12.

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)#
```

20. DHCP Relay Commands

20-1 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	Specify the address pool name with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In addition to DHCP relay packets, based on the **ip helper-address** command, 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, 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. Otherwise, the packet is relayed based on the IP helper-address configured on the received interface. 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 a DHCP relay pool, called pool1, is created. 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)#
```

20-2 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 the 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.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the DHCP service 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)#
```

20-3 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 the command to remove the configuration for the interface.

ip dhcp relay information check-reply [none]

no ip dhcp relay information check-reply

Parameters

none	Specifies to disable check for Option 82 of the reply packet.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the DHCP service 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 enables the DHCP relay agent check for the VLAN 100. The effect state of the check function for VLAN100 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
```

20-4 ip dhcp relay information option

This command is used to enable the insertion of relay agent information (Option 82) during the relay of DHCP request packets. Use the **no** command to 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.

Command Default Level

Level: 12.

Usage Guideline

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 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)#
```

20-5 ip dhcp relay information option-insert

This command is used to enable or disable the insertion of Option 82 for an interface during the relay of DHCP request packets. Use the **no** command to remove the configuration of the insert function for the interface.

ip dhcp relay information option-insert [none]

no ip dhcp relay information option-insert

Parameters

none	Specifies to disable insertion of Option 82 in the relayed packet.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the DHCP service is enabled.

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)#
```

20-6 ip dhcp relay information policy

This command is used to configure the Option 82 re-forwarding policy for the DHCP relay agent. Use the **no** form of the command to restore 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.

Command Default Level

Level: 12.

Usage Guideline

The command only takes effect when the DHCP service 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. If the **ip dhcp relay information relay** command is configured in the global configuration mode but not configured in the interface configuration mode, the global configuration is applied to all interfaces.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information policy keep
Switch(config)#
```

20-7 ip dhcp relay information policy-action

This command is used to configure the information re-forwarding policy for the DHCP relay agent for an interface. Use the **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

The command only takes effect when the DHCP service 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 and set the policy to drop for VLAN 100. The effective relay agent option re-forwarding policy for VLAN 100 is drop and the effective relay agent option re-forwarding policy 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)#
```

20-8 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 the command to configure the default remote ID sub-option.

ip dhcp relay information option format remote-id {default | string *STRING* **| vendor2}**

no ip dhcp relay information option format remote-id

Parameters

default	Specifies to use the switch's system MAC address as the remote ID.
STRING	Specifies to use a user-defined string as the remote ID. Space characters are allowed in the string.
vendor2	Specifies user the vendor 2.

Default

The switch's system MAC address is used as the remote ID string.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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# 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)#
```

20-9 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 the command to configure the default circuit ID sub-option.

ip dhcp relay information option format circuit-id {default | string *STRING* **| vendor1}**

no ip dhcp relay information option format circuit-id

Parameters

default	Specifies to use the default circuit ID sub-option.
STRING	Specifies to use a user-defined string as the circuit ID. Space characters are allowed in the string.
vendor1	Specifies to use vender1.

Default

The circuit ID format is VLAN ID, module number and port number.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

20-10 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** 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.

Command Default Level

Level: 12.

Usage Guideline

When IP DHCP relay information trust option 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’s setting is enabled, IP DHCP relay information is trusted for all interfaces. When this command’s setting is disabled, the trust state is determined by the interface mode command **ip dhcp relay information trusted**.

Verify settings by entering the **show ip dhcp relay information trusted-sources** command.

Example

This example shows how to enable the DHCP relay agent to trust IP DHCP relay information for all interfaces. The DHCP relay agent trusts the relay information for all interfaces regardless of what the setting of **ip dhcp relay information trusted** command.

```
Switch# configure terminal
Switch(config)# ip dhcp relay information trust-all
Switch(config)#
```

20-11 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** 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.

Command Default Level

Level: 12.

Usage Guideline

When IP DHCP relay information is trusted on an interface, the arriving packets with the 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 setting is enabled, IP DHCP relay information is trusted for all interfaces. When this command setting is disabled, the trust state is determined by the interface mode command **ip dhcp relay information trusted**.

Verify the settings by entering the **show ip dhcp relay information trusted-sources** command.

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)#
```

20-12 ip dhcp local-relay vlan

This command is used to enable local relay on a VLAN or a group of VLANs. Use the **no** command to disable the local relay function.

ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

no ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

Parameters

vlan *VLAN-ID*	Specifies the VLAN used.

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

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

20-13 relay destination

This command is used to specify the DHCP relay destination IP address associated with a relay pool. Use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

In addition to the relay DHCP packet based on **ip helper-address**, 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 anyone of the relay sources, the packet will be forwarded to all of the relay destinations.

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 this relay pool. Otherwise, the packet is relayed based on the IP helper address configured for the received interface. 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 a DHCP relay pool “pool1” is created. In the relay pool, the subnet 172.19.10.0/255.255.255.0 is specified as the source subnet and 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)#
```

20-14 relay source

This command is used to specify the source subnet of client packets. Use the **no** form of 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.

Command Default Level

Level: 12.

Usage Guideline

In addition to relay DHCP packets based on the **ip helper-address** command, the relay destination of DHCP server can be specified in 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. Multiple relay sources and multiple relay destinations can be specified in a pool. If a packet matches anyone of the relay source, 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 rely source of a relay pool, the packet will be relayed based on this relay pool. Otherwise, the packet is relayed based on the IP helper address configured on the received interface. 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, if the interface that receives the packet has no IP address configured.

Example

This example shows how a DHCP relay pool “pool2” is created. 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)#
```

20-15 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 the 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 Class Configuration Mode.

Command Default Level

Level: 12.

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, then 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, if 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)#
```

20-16 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the effective setting of the trust relay information option function.

Example

This example shows how to use this command. Note that the display output lists the interfaces that are configured to be trusted sources.

```
Switch# show ip dhcp relay information trusted-sources

List of trusted sources of relay agent information option:
vlan100             vlan200             vlan300             vlan400
vlan500

Switch#
```

This example shows how to display when all interfaces are trusted sources. Note that the display output does not list the individual interfaces.

```
Switch# show ip dhcp relay information trusted-sources
```

```
All interfaces are trusted source of relay agent information option

Switch#
```

20-17 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display relay information options with insert configuration information.

Example

This example shows how to displays 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#
```

20-18 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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: 3

Switch#
```

21. DHCP Server Commands

21-1 address range

This command is used to specify an IP address range to be associated with a DHCP class in a DHCP address pool. Use the **no** form of the command to remove the address range to be associated with a DHCP class.

address range *START-IP-ADDRESS END-IP-ADDRESS*

no address range *START-IP-ADDRESS END-IP-ADDRESS*

Parameters

START-IP-ADDRESS	Specifies the address or the first address in a range of addresses.
END-IP-ADDRESS	Specifies the last address in a range of addresses.

Default

None.

Command Mode

DHCP Pool Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **address range** command and the **class** command in a DHCP address pool to restrict the allocation of IP address from a subnet in the address pool. The network for allocating addresses is partitioned based on the DHCP option value of the request. If an address pool has classes defined, the allocation of address will based on the class from this address pool if the IP DHCP use class setting is enabled.

When the server attempts to allocate an address from an address pool and if the address pool has classes defined, the server will check first whether the pool contains the subnet appropriate for the request. If the subnet of the address pool contains the GIADDR (if not zero) or the subnet of the received interface, then the server will directly matching the class definition of the address pool to allocate the address. The server will only allocate an address from the matched class.

To remove an address range, only the exact range of addresses that are previously configured can be specified.

Example

This example shows how a DHCP class “Customer-A” is created with the relay information option matching pattern. They are associated with an address range in the DHCP address pool “pool1”.

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)#
```

21-2 bootfile

This command is used to specify the configuration file or image file for the DHCP client to boot the device. Use the **no** command to remove the specification of the boot file.

boofile *URL*

no bootfile

Parameters

URL	Specifies the boot file URL. This URL can be up to 64 characters long.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the configuration file or the image file for the DHCP client to boot the device. The **next-server** command specifies the location of the server where the boot file resides.

Example

This example shows how to specify “mdubootfile.bin” as the name of the boot file for DHCP pool 1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# bootfile \bootimage\mdubootfile.bin
Switch(config-dhcp-pool)#
```

21-3 clear ip dhcp binding

This command is used to delete the address binding entry from the DHCP server database.

clear ip dhcp {all | pool *NAME***} binding [vrf** *VRF-NAME***] {* | *IP-ADDRESS***}**

Parameters

all	Specifies to clear the binding entries for all pools.
pool *NAME*	Specifies the name of the DHCP pool.
vrf *VRF-NAME*	(Optional) Specifies to clear the binding entry in the specified VRF.
*	Specifies to clear all binding entries associated with the specified pool.
IP-ADDRESS	Specifies the IP address of the binding entry to be deleted.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to delete the binding of addresses. If **pool** is specified but the IP address is specified as *, then all automatic binding entries associated with the pool will be deleted. If **pool** is specified as all and the IP address is specified, then the automatic binding entry specific to the IP address will be deleted regardless of the pool that contains the binding entry. If both **pool** and the IP address are specified, then the automatic entry of the specified IP address in the specific pool will be cleared.

Example

This example shows how to delete the address binding 10.12.1.99 from the DHCP server database.

```
Switch# clear ip dhcp all binding 10.12.1.99
Switch#
```

This example shows how to delete all bindings from all pools.

```
Switch# clear ip dhcp all binding *
Switch#
```

This example shows how to delete address binding 10.13.2.99 from the address pool named pool 2.

```
Switch# clear ip dhcp pool pool2 binding 10.13.2.99
Switch#
```

21-4 clear ip dhcp conflict

This command is used to clear the DHCP conflict entry from the DHCP server database.

clear ip dhcp {all | pool *NAME***} conflict [vrf** *VRF-NAME***] {* |** *IP-ADDRESS***}**

Parameters

all	Specifies to clear conflict entries for all pools.
pool *NAME*	Specifies the name of the DHCP pool.
vrf *VRF-NAME*	(Optional) Specifies to clear DHCP conflict entries in the specified VRF.
*****	Specifies to clear all conflict entries associated with the specified pool.
IP-ADDRESS	Specifies the IP address of the conflict entry to be deleted.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to delete the address from the conflict table. The deleted address will be returned to the address pool and free to be assigned. The DHCP server detects the conflict of an IP address by using a ping operation.

If **pool** is specified but the IP address is specified as *, then all conflict entries specific to the pool will be deleted. If **pool** is specified as all and the IP address is specified, then the specified conflict entry will be deleted regardless of the pool that contains the conflict entry. If both **pool** and the IP address are specified, then the specified conflict entry specific to the specific pool will be cleared.

Example

This example shows how to clear an address conflict of 10.12.1.99 from the DHCP server database.

```
Switch# clear ip dhcp all conflict 10.12.1.99
Switch#
```

This example shows how to delete the all conflict addresses from the DHCP server database.

```
Switch# clear ip dhcp all conflict *
Switch#
```

This example shows how to delete all address conflicts from the address pool named pool 1.

```
Switch# clear ip dhcp pool pool1 conflict *
Switch#
```

This example shows how to delete an address conflict 10.13.2.99 from the address pool named pool 2.

```
Switch# clear ip dhcp pool pool2 conflict 10.13.2.99
Switch#
```

21-5 clear ip dhcp server statistics

This command is used to reset all DHCP server counters.

clear ip dhcp server statistics

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear all of DHCP statistic counters.

Example

This example shows how to reset all DHCP counters to zero.

```
Switch# clear ip dhcp server statistics
Switch#
```

21-6 class (DHCP relay & server)

This command is used to enter the DHCP Pool Configuration Mode and to associate a range of IP addresses with the DHCP class. Use the **no** form of the command to remove the association.

class *NAME*

no class *NAME*

Parameters

NAME	Specifies the DHCP class name. This name can be up to 32 characters long.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

Use the **address range** command and the **class** command in a DHCP address pool to restrict the allocation of IP address from subnet in the address pool. Thus, the network for allocating addresses is partitioned based on the DHCP option value of the request.

If an address pool has classes defined, the allocation of addresses from this address pool will based on the class if the IP DHCP use class setting is enabled.

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

Example

This example shows how two DHCP classes Customer-A and Customer-B are created with option matching patterns. They are associated with address ranges in the DHCP server address pool “srv-pool1”.

```
Switch# configure terminal
Switch(config)# ip dhcp class Customer-A
Switch(config-dhcp-class)# option 82 hex 1234 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Customer-B
```

```
Switch(config-dhcp-class)# option 82 hex 5678 *
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool srv-pool1
Switch(config-dhcp-pool)# network 172.28.5.0/24
Switch(config-dhcp-pool)# class Customer-A
Switch(config-dhcp-pool-class)# address-range 172.28.5.1 172.28.5.12
witch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Customer-B
Switch(config-dhcp-pool-class)# address-range 172.28.5.18 172.28.5.32
Switch(config-dhcp-pool-class)#
```

This example shows how a DHCP class Service-A is configured and defined with a DHCP Option 60 matching pattern 0x112233 and 0x102030. Another class Service-B is configured and defined with a DHCP Option 60 matching pattern 0x556677 and 0x506070. A class Default-class is configured with no option hexadecimal command. These defined classes are used in the relay pool “pool1”. The class Service-A is associated with relay target 10.2.1.2 and the class Service-B is associated with relay target 10.2.1.5. The class Default-class is associated with the relay target 10.2.1.32.

```
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 class Service-B
Switch(config-dhcp-class)# option 60 hex 556677
Switch(config-dhcp-class)# option 60 hex 506070
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Default-class
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# relay source 172.19.18 255.255.255.0
Switch(config-dhcp-pool)# class Service-A
Switch(config-dhcp-pool-class)# relay target 10.2.1.2
Switch(config-dhcp-pool-class)# exit
Switch(config-dhcp-pool)# class Service-B
Switch(config-dhcp-pool-class)# relay target 10.2.1.5
Switch(config-dhcp-pool)# exit
Switch(config-dhcp-pool)# class Default-class
Switch(config-dhcp-pool-class)# relay target 10.2.1.32
Switch(config-dhcp-pool)#
```

21-7 client-identifier

This command is used to specify the unique DHCP client ID of the manual binding entry in a DHCP address pool. Use the **no** command to remove the specification of the client identifier.

client-identifier *IDENTIFIER*

no client-identifier

Parameters

IDENTIFIER	Specifies a DHCP client identifier in hexadecimal notation.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is valid for manual binding entries in a DHCP address pool. The client identifier is formatted by media type and the MAC address. Only one manual binding entry can be specified in a DHCP address pool. With a manual binding entry, the IP address can be either be bound with a client-identifier or bound with the hardware address of the host.

Use the **client-identifier** command and the **host** command to specify the manual binding entry based on the client-identifier in the DHCP packet.

Example

This example shows how a DHCP address pool “pool1” is created with a manual binding entry which binds the IP address 10.1.2.3/24 with client ID 0x01524153203124.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# client-identifier 01524153203124
Switch(config-dhcp-pool)# host 10.1.2.3/24
Switch(config-dhcp-pool)#
```

21-8 default-router

This command is used to specify default routers for the DHCP client. Use the **no** form of this command to remove the default router.

default-router *IP-ADDRESS* **[***IP-ADDRESS2***...***IP-ADDRESS8***]**

no default-router *IP-ADDRESS* **[***IP-ADDRESS2***...***IP-ADDRESS8***]**

Parameters

IP-ADDRESS	Specifies the IP address of the default router for the DHCP client.
*IP-ADDRESS2***...***IP-ADDRESS8*	Specifies multiple IP addresses, separated by spaces. Up to eight addresses can be specified.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the default routers for the clients. The IP address of the router should be on the same subnet as the client's subnet. Routers are listed in the order of preference. If default routers are already configured, the default routers configured later will be added to the default interface list.

Example

This example shows how to specify 10.1.1.1 as the IP address of the default router in the DHCP address pool.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# default-router 10.1.1.1
```

21-9 domain-name

This command is used to specify the domain name for a DHCP client. Use the **no** form of this command to remove the domain name.

domain-name *NAME*

no domain-name

Parameters

NAME	Specifies the domain name. This name can be up to 64 characters long.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command configures the domain name for the DHCP client. Only one domain name can be specified.

Example

This example shows how to specify the domain name as domain.com in the DHCP address pool.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# domain-name domain.com
```

21-10 dns-server

This command is used to specify DNS servers for the DHCP client. Use the **no** form of this command to remove the specific DNS server

dns-server *IP-ADDRESS* **[***IP-ADDRESS2***…***IP-ADDRESS8***]**

no dns-server *IP-ADDRESS* **[***IP-ADDRESS2***…***IP-ADDRESS8***]**

Parameters

IP-ADDRESS	Specifies an IP addresses to be used by the DHCP client as the DNS server.
*IP-ADDRESS2***…***IP-ADDRESS8*	Specifies multiple IP addresses, separated by spaces. Up to eight servers can be specified.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to configure the IP address that will be used by the client as the DNS server. Up to eight servers can be specified. Servers are listed in the order of preference. If DNS servers are already configured, the DNS servers configured later will be added to the DNS server list.

Example

This example shows how to specify 10.1.1.1 as the IP address of the DNS server in the DHCP address pool.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# dns-server 10.1.1.1
```

21-11 hardware-address

This command is used to specify the hardware address of the manual binding entry in the DHCP address pool. Use the **no** command to remove the specification of the hardware address of the manual binding entry.

hardware-address *HARDWARE-ADDRESS*

no hardware-address

Parameters

HARDWARE-ADDRESS	Specifies the MAC address of the client.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A binding entry is a mapping between the IP address and the hardware address or the client identifier. By creating a manual binding entry, an IP address is manually assigned to a client.

Only one manual binding entry can be specified in a DHCP address pool. With a binding entry, the IP address can be either bound with a client identifier or bound with the hardware address of the host.

Use the **client-identifier** command and the **host** command to specify the manual binding entry based on client identifier in the DHCP packet. Use the **hardware-address** command and the **host** command to specify the manual binding entry based on hardware address.

Example

This example shows how a DHCP address pool “pool1” is created with a manual binding entry which binds the IP address 10.1.2.100/24 with the MAC address C2:F3:22:0A:12:F4.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2F3.220A.12F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

21-12 host

This command is used to specify the IP address of the manual binding entry in a DHCP address pool. Use the **no** command to remove the specification of the IP address from the entry.

host {*IP-ADDRESS MASK* **|** *IP-ADDRESSIPREFIX-LENGTH***}**

no host

Parameters

IP-ADDRESS	Specifies the IP address of the manual binding entry.
MASK	Specifies the bits that mask the network part of the host address.
PREFIX-LENGTH	Specifies the prefix length of the network. It is an alternative way to specify the network mask.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only one binding entry can be specified in a DHCP address pool. In a binding entry, the IP address can be either bound with a client identifier or bound with the hardware address of the host.

Use the **client-identifier** command with the **host** command to specify the manual binding entry based on client identifier. Use the **hardware-address** command with the **host** command to specify the manual binding entry based on hardware address.

Example

This example shows how a DHCP address pool “pool1” is created with a manual binding entry which binds the IP address 10.1.2.100/24 with the MAC address C2:F3:22:0A:12:F4.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# hardware-address C2:F3:22:0A:12:F4
Switch(config-dhcp-pool)# host 10.1.2.100/24
Switch(config-dhcp-pool)#
```

21-13 ip dhcp class (DHCP Relay & Server)

This command is used to define a DHCP class and enter the DHCP class configuration mode. Use the **no** form of the command to remove a DHCP class.

ip dhcp class *NAME*

no ip dhcp class *NAME*

Parameters

NAME	Specifies the DHCP class name. This name can be up to 32 characters long.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the DHCP class configuration mode and then use the **option hex** command to define the option matching pattern for the DHCP class. When a class has no option hexadecimal associated, the class will be matched by any packet.

Example

This example shows how a DHCP class Service-A is configured and defined with a 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)#
```

21-14 ip dhcp excluded-address

This command is used to exclude a range of IP addresses from being allocated to the client. Use the **no** form of the command to remove a range of excluded addresses.

ip dhcp excluded-address [vrf *VRF-NAME***]** *START-IP-ADDRESS END-IP-ADDRESS*

no ip dhcp excluded-address [vrf *VRF-NAME***]** *START-IP-ADDRESS END-IP-ADDRESS*

Parameters

VRF-NAME	(Optional) Specifies to exclude IP addresses from the virtual routing and forwarding (VRF) space. If no VRF is specified, it creates the excluded address for the global routing and forwarding space.
START-IP-ADDRESS	Specifies an address or the first address of a range of addresses to be excluded.
END-IP-ADDRESS	Specifies the last address of a range of addresses to be excluded.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The DHCP server automatically allocates addresses in DHCP address pools to DHCP clients. All the addresses except the interface's IP address on the router and the excluded address specified by the **ip dhcp excluded-address** command are available for allocation. Multiple ranges of addresses can be excluded. To remove a range of excluded addresses, administrators must specify the exact range of addresses previously configured.

Example

This example shows how the range of addresses 10.1.1.1 to 10.1.1.255 and 10.2.1.1 to 10.2.1.255 are excluded.

```
Switch# configure terminal
Switch(config)# ip dhcp excluded-address  10.1.1.1 10.1.1.255
Switch(config)# ip dhcp excluded-address  10.2.1.1 10.2.1.255
```

21-15 ip dhcp ping packets

This command is used to specify the number of packets that the DHCP server will send as a part of the ping operation. Use the **no** command to restore the default number.

ip dhcp ping packets *COUNT*

no ip dhcp ping packets

Parameters

COUNT	Specifies the number of ping packets that the DHCP server will send.

Default

By default, this value is 2.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the number of packets that the DHCP server will send as part of the ping operation. The DHCP server performs the ping operation to detect whether there is a conflict in use of the IP address before assigning an IP address to the client. If there is no response after the specified number of attempts, the IP address will be assigned to the client, and it becomes an entry. If the server receives a response to the ping operation, the IP address will become a conflict entry.

Setting the number to 0 will disable the ping operation.

Example

This example shows how to configure the number of ping packets as 3.

```
Switch# configure terminal
Switch(config)# ip dhcp ping packets 3
Switch(config)#
```

21-16 ip dhcp ping timeout

This command is used to specify the time the DHCP server should wait for the ping reply packet. Use the **no** form of this command to restore the default value.

ip dhcp ping timeout *MILLI-SECONDS*

no ip dhcp ping timeout

Parameters

MILLI-SECONDS	Specifies the interval of time the DHCP server will wait for the ping reply. The maximum timeout is 10000 milliseconds (10 seconds). The specified value should be multiples of 100.

Default

By default, this value is 100 milliseconds (0.1 seconds).

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the timeout length for the ping operation. The DHCP server performs the ping operation to an IP address to detect whether there is a conflict in the use of the IP address before assigning the IP address to a client. If there is no response after the specified number of attempts, the IP address will be assigned to the client, and it becomes an entry. If the server receives a response to the ping operation, the IP address will become a conflict entry.

Example

This example shows how to configure the waiting time for a ping reply.

```
Switch# configure terminal
Switch(config)# ip dhcp ping timeout 800
Switch(config)#
```

21-17 ip dhcp pool (DHCP Server)

This command is used to configure a DHCP address pool on the DHCP server and enter the DHCP Pool Configuration Mode. Use the **no** form of this command to remove a DHCP address pool.

ip dhcp pool *NAME*

no ip dhcp pool *NAME*

Parameters

NAME	Specifies the name of the address. This name can be up to 32 characters long.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A DHCP server receives requests from DHCP clients and services and then allocates an IP address from the address pool and replies the address to the client. An address pool can either contain a network of IP addresses or a single IP address. Use the **network** command in the DHCP Pool Configuration Mode to specify a network for the address pool or use the **client-identifier** or **hardware-address** command with the **host** command to specify a manual binding entry in a DHCP address pool.

Example

This example shows how a DHCP address pool “pool1” is created.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)#
```

21-18 ip dhcp use class (DHCP Relay & Server)

This command is used to specify the DHCP server to use DHCP classes during address allocation or the DHCP relay agent to use DHCP classes to locate the relay destination addresses. Use the **no** command to disable the use of DHCP classes.

ip dhcp use class

no ip dhcp use class

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the DHCP server to use DHCP classes during address allocation or the DHCP relay agent to use DHCP classes to locate the relay destination addresses. Use the **no** command to disable the use of DHCP classes.

Example

This example shows how use of the DHCP class is disabled.

```
Switch# configure terminal
Switch(config)# no ip dhcp use class
Switch(config)#
```

21-19 lease

This command is used to configure the duration of the lease for an IP address that is assigned from the address pool. Use the **no** form of this command to restore the default setting.

lease {*DAYS* **[***HOURS* **[***MINUTES***]] | infinite}**

no lease

Parameters

DAYS	Specifies the number of days for the duration of the lease.
HOURS	(Optional) Specifies the number of hours for the duration of the lease.
MINUTES	(Optional) Specifies the number of minutes for the duration of the lease.
infinite	Specifies that the lease time is unlimited.

Default

By default, the lease time is 1 day.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the duration of the lease for an IP address that is assigned from the address pool. The least setting will not be inherited from the parent address pool.

Example

This example shows how to configure the lease in the address pool “pool1” to 1 day.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 1
```

This example shows how to configure the lease in the address pool “pool1” to 1 hour.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# lease 0 1
```

21-20 netbios-node-type

This command is used to configure the NetBIOS node type for Microsoft DHCP clients. Use the **no** form of this command to remove the configuration of the NetBIOS node type.

netbios-node-type *NTYPE*

no netbios-node-type

Parameters

NTYPE	Specifies the NetBIOS node type of the Microsoft client. The following are the valid types: • **b-node:** Broadcast • **p-node:** Peer-to-peer • **m-node:** Mixed • **h-node:** Hybrid

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the NetBIOS node type of the Microsoft DHCP client. The node type of the h-node (Hybrid) is recommended. The node type determines the method NetBIOS use to register and resolve names. The broadcast system uses broadcasts. A p-node system uses only point-to-point name queries to a name server (WINS). An m-node system broadcasts first, and then queries the name server. A hybrid system queries the name server first, and then broadcasts.

Example

This example shows how to configure the NetBIOS node type as h-node.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# netbios-node-type h-node
Switch(config-dhcp-pool)#
```

21-21 netbios-name-server

This command is used to specify WINS name servers for the Microsoft DHCP client. Use the **no** form of this command to remove the configuration of specific WINS servers.

netbios-name-server *IP-ADDRESS* **[***IP-ADDRESS2***…***IP-ADDRESS8***]**

no netbios-name-server *IP-ADDRESS* **[***IP-ADDRESS2***…***IP-ADDRESS8***]**

Parameters

IP-ADDRESS	Specifies the WINS name server IP address for the DHCP client.
*IP-ADDRESS2***…***IP-ADDRESS8*	Specifies multiple IP addresses, separated by spaces. Up to eight servers can be specified.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the WINS name server IP addresses that that are available to the Microsoft client. Up to eight servers can be specified. Servers are listed in the order of preference. If name servers are already configured, the name server configured later will be added to the default interface list.

Example

This example shows how to configure 10.1.1.100 and 10.1.1.200 as WINS servers for the address pool “pool1”.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# netbios-name-server 10.1.1.100 10.1.1.200
Switch(config-dhcp-pool)#
```

21-22 next-server

This command is used to specify the BOOT server for the DHCP client. Use the **no** form of this command to remove boot servers.

next-server *IP-ADDRESS*

no next-server

Parameters

IP-ADDRESS	Specifies the boot server IP address for the client to get the boot file.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the server IP address for the client to boot the image. The server is typically a TFTP server. Only one boot server can be specified.

Example

This example shows how to configure 10.1.1.1 as the IP address of next server in the DHCP client's boot process in the pool named pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# next-server 10.1.1.1
```

21-23 network

This command is used to configure the network with its associated mask for a DHCP address pool. Use the **no** command to remove the network.

network {*NETWORK-ADDRESS MASK* **|** *NETWORK-ADDRESSIPREFIX-LENGTH***}**

no network

Parameters

NETWORK-ADDRESS	Specifies the network address for the address pool.
MASK	Specifies the bits that mask the network part of the address.
PREFIX-LENGTH	Specifies the prefix length of the network. It is an alternative way to specify the network mask.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the DHCP Pool Configuration Mode to configure a network for the address pool. The user cannot configure the manual binding entry in the address pool that was configured with the network.

When the DHCP server receives a request from a client, the server will select an address pool or subnet in the address pool based on the following rules for address allocation. When an IP address is allocated to a host, a binding entry is created.

- If the client is not directly connected to the DHCP server, the discover message is relayed by the relay agent. The server will select the address pool configured with a subnet that contains the GIADDR of the packet. If an address pool is selected, the server will try to allocate the address from the subnet.
- If the client is directly connected to the server, then the server will look for the subnet of the address pool that contains or match the primary subnet of the received interface. If not found, the server will look for the subnet of the address pool that contains or match the secondary subnet of the received interface.

If an address is allocated from a specific subnet, the network mask associated with the subnet will be replied as the network mask to the user. The network configured for a DHCP address pool can be a natural network or a sub-network. The configured DHCP address pools are organized as a tree. The root of the tree is the address pool that contains the natural network. The address pools that contain the sub-network are branches under the root, and the address pools that contain the manual binding entry is the leave under the branch or under the root. Based on the tree structure, the child address pool will inherit the attributes configured for its parent address pool. The only exception to this inheritance is lease attribute.

Example

This example shows how the subnet 10.1.0.0/16 is configured for the DHCP address pool pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# network 10.1.0.0/16
Switch(config-dhcp-pool)# default-router 10.1.1.1
Switch(config-dhcp-pool)#
```

21-24 option

This command is used to configure DHCP server options. Use the **no** form of this command to remove a specific option.

option *CODE* **{ascii** *STRING* **| hex {***HEX-STRING* **| none} | ip** *IP-ADDRESS* **[***IP-ADDRESS2***…***IP-ADDRESS8***]}**

no option *CODE*

Parameters

CODE	Specifies the DHCP option number in decimals.
ascii *STRING*	Specifies an ASCII string for the DHCP option with a maximum of 255 bytes.
hex {*HEX-STRING***}**	Specifies the hexadecimal format for the DHCP option with a maximum of 254 characters. *HEX-STRING***:** Specifies the hexadecimal string for the DHCP option. **none:** Specifies the zero-length hexadecimal string.

ip *IP-ADDRESS*	Specifies the IP addresses. Up to eight IP addresses can be specified.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command configures DHCP options in a DHCP pool. DHCP options can also be configured by other commands such as the **default-router** command in the DHCP Pool Configuration Mode. The DHCP server will carry all the configured DHCP options in all reply packets. All of the configured DHCP options will be carried in the DHCP packet replied by the server.

The length of the configured hexadecimal string must be even (For example, 001100 is correct and 11223 is incorrect). Only one string can be specified for the same option number.

There is a restriction on the total length of DHCP options. The restriction may be specified by the client or determined by the server if the client didn't specify this. If not specified, then the maximum length is 312.

The following options can be configured by other DHCP pool configuration mode commands and should not be configured by the option command.

- Option 1 (Subnet Mask, configured by the network).
- Option 3 (Router Option, configured by the default router).
- Option 6 (Domain Name Server, configured by the DNS server).
- Option 15 (Domain Name, configured by the domain name).
- Option 44 (NetBIOS Name Server, configured by the NetBIOS name server).
- Option 46 (NetBIOS Node Type, configured by the NetBIOS node type).
- Option 51 (IP Address Lease Time, configured by the lease).
- Option 58 (Renewal (T1) Time Value, configured by the lease).
- Option 59 (Rebinding (T2) Time Value, configured by the lease).

The following options cannot be configured through this command:

- Option 12 (Host name default option).
- Option 50 (Requested address, default option).
- Option 53 (DHCP Message Type, default option).
- Option 54 (Server Identifier, default option).
- Option 55 (Parameter request list, default option).
- Option 61 (Client Identifier, default option).
- Option 82 (Relay agent information option, default option).

Example

This example shows how to specify the DHCP server Option 69 (SMTP server option) in the hexadecimal format. The hexadecimal string is c0a800fe (192.168.0.254).

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# option 69 hex c0a800fe
```

This example shows how to specify the DHCP server Option 40 (the name of the client's NIS domain) in the ASCII string format.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# option 40 ascii net.market
```

This example shows how to specify the DHCP server Option 72 (WWW server option) in the IP format. Two WWW servers are configured, 172.19.10.1 and 172.19.10.100.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(dhcp-config)# option 72 ip 172.19.10.1 172.19.10.100
```

21-25 option hex (DHCP Relay & Server)

This command is used to specify a DHCP option matching pattern for a DHCP class. Use the **no** 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 hexadecimal pattern of the specified DHCP option.
*****	Specifies the remaining bits of the option that will not be matched. If * is not specified, the bit length of the pattern should be the same as the bit length of the option.
MASK	Specifies the hexadecimal bit mask for the masking of the pattern. The masked pattern bits will be matched. If the mask is not specified, all the bits specified by the pattern will be checked. The bit set as 1 will be checked. The input format should be the same as the pattern.

Default

None.

Command Mode

DHCP Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The user can use the **ip dhcp class** command with the **option hex** command to define a DHCP class. The classes in a pool are matched in the order that the class is configured in a pool.

With the **option hex** command, the user can 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 patterns of a DHCP class, the packet will be classified to the DHCP class and forwarded based on the specified target.

The following are some commonly used option codes:

- Option 60 (Vendor Class Identifier).
- Option 61 (Client Identifier).
- Option 77 (User Class).
- Option 82 (Relay Agent Information Option).
- Option 124 (Vendor-identifying Vendor Class).
- Option 125 (Vendor-identifying Vendor-specific Information).

Example

This example shows how a DHCP class Service-A is configured and defined with the DHCP Option 60 matching pattern 0x112233 and 0x102030. Another class Service-B is configured and defined with the DHCP Option 60 matching pattern 0x5566* and 0x5060*.

```
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 class Service-B
Switch(config-dhcp-class)# option 60 hex 5566*
Switch(config-dhcp-class)# option 60 hex 5060*
Switch(config-dhcp-class)# exit
Switch(config)# ip dhcp class Service-B
Switch(config-dhcp-class)#
```

21-26 service dhcp

This command is used to enable the DHCP server and relay service on the switch. Use the **no** form of this command to disable the DHCP server and relay service.

service dhcp

no service dhcp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the DHCP server and relay service on the switch.

Example

This example shows how to disable the DHCP server and relay service.

```
Switch# configure terminal
Switch(config)# no service dhcp
Switch(config)#
```

21-27 show ip dhcp binding

This command is used to display the address binding entries on the DHCP Server.

show ip dhcp binding [vrf *VRF-NAME***] [***IP-ADDRESS***]**

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.
IP-ADDRESS	(Optional) Specifies the binding entry to display. If the IP address is not specified, all binding entries or the binding entry specific to the specified pool are displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The IP address, hardware address, lease start and lease expiration of the entry will be displayed.

Example

This example shows how to display the binding status of al bound IP addresses.

```
Switch# show ip dhcp binding

VRF Name: vrf1
IP address     Client-ID/              Lease expiration       Type
               Hardware address
----------     ----------------     ---------------------  -----------
10.1.1.1       0100b810863212        Oct 23 2013 09:12 AM   Automatic
10.1.9.1       0100b7443dc224        Oct 23 2013 01:12 AM   Automatic
10.1.11.10     0100b22291226d        infinite               Manual

Switch#
```

This example shows how to display the binding status of IP address 10.1.1.1 in the DHCP address pool.

```
Switch# show ip dhcp binding 10.1.1.1

VRF Name: vrf1
IP address     Client-ID/              Lease expiration       Type
               Hardware address
----------     ----------------     --------------------    -------
10.1.1.1       0100bc2394625b     Oct 23 2013 09:12 AM    Automatic

Switch#
```

21-28 show ip dhcp conflict

This command is used to display the conflict IP addresses while the DHCP Server attempts to assign the IP address for a client.

show ip dhcp conflict [vrf *VRF-NAME*] [*IP-ADDRESS*]

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.
IP-ADDRESS	(Optional) Specifies the conflict entry to display. If the IP address is not specified, all conflict entries or the conflict entry specific to the specified pool are displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The DHCP server detects the conflict of IP addresses by using the ping operation. If a conflict address is found, then this IP address will be removed from the address pool and marked as a conflict. The conflict address will not be assigned until the network administrator clears the conflict address.

Example

This example shows how to display the conflict status of the IP address 10.1.1.1.

```
Switch# show ip dhcp conflict 10.1.1.1

IP address     Detected Method    Detection time        VRF
----------     ----------------   -------------------   -----
10.1.1.1       Ping               Oct 23 2013 09:12 AM  vrf1

Switch#
```

This example shows how to display the conflict status of all DHCP IP addresses in the pool.

```
Switch# show ip dhcp conflict

IP address     Detected Method    Detection time        VRF
----------     ----------------   -------------------   -----
10.1.1.1       Ping               Oct 23 2013 09:12 AM  vrf1

Switch#
```

This example shows how to display the conflict status of the IP address 10.1.1.1.

```
Switch# show ip dhcp conflict pool vrf vrf1

IP address     Detected Method    Detection time        VRF
----------     ----------------   -------------------   -----
10.1.1.1       ping               Oct 23 2013 09:12 AM  vrf1
```

```
Switch#
```

21-29 show ip dhcp pool

This command is used to display information about the DHCP pools.

show ip dhcp pool [*NAME***]**

Parameters

NAME	(Optional) Specifies to display information about a specific DHCP pool. If not specified, information about all DHCP pools will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to examine the configuration settings of the pool or all the pools if the name parameter is not used.

Example

This example shows how to display the DHCP pool “pool1” configuration information.

```
Switch# show ip dhcp pool1

Pool name: pool1
  VRF Name: vrf1
  Network: 172.28.5.0/24
  Boot file: boot.bin
  Default router: 10.1.2.1
  DNS server: 10.1.2.1
  NetBIOS server: 10.1.2.3
  Domain name: alphanetworks.com
  Lease: 1 days 3 hours 20 minutes
  NetBIOS node type: hybrid
  Next server: 10.1.2.1
  class Customer-A
  address-range 172.28.5.1 172.28.5.12
  class Customer-B
  address-range 172.28.5.18 172.28.5.32

Remaining unallocated address number: 511
Number of leased address: 100

Switch#
```

21-30 show ip dhcp server

This command is used to display the current status of the DHCP server.

show ip dhcp server

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the DHCP server status and user configured address pool.

Example

This example shows how to display the status of the DHCP server.

```
Switch# show ip dhcp server

DHCP Service: Disable
Ping packets number: 3
Ping timeout: 500 ms
Excluded Addresses
10.1.1.1-10.1.1.255

List of DHCP server configured address pool
pool1               pool2               pool3               pool4
pool5               pool6               pool7               pool8
pool9               pool10              pool11              pool12

Switch#
```

21-31 show ip dhcp server statistics

This command is used to display DHCP server statistics.

show ip dhcp server statistics

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays DHCP counters. All counters are cumulative.

Example

This example shows how to display DHCP server statistics.

```
Switch# show ip dhcp server statistics

Address pools              3
Automatic bindings         100
Manual binding             2
Malformed messages         0
Renew messages             0

Message             Received
BOOTREQUEST                12
DHCPDISCOVER               200
DHCPREQUEST                178
DHCPDECLINE                0
DHCPRELEASE                0
DHCPINFORM                 0

Message                 Sent
BOOTREPLY               12
DHCPOFFER               190
DHCPACK                 172
DHCPNAK                  6

Switch#
```

Display Parameters

Address pools	The number of configured address pools in the DHCP database.
Malformed messages	The number of truncated or corrupted messages that were received by the DHCP server.
Renew messages	The number of renewed messages for a DHCP lease. The counter is incremented when a new renew message has arrived after the first renew message.
Message	The DHCP message type.
Received	The number of DHCP messages that were received by the DHCP server.
Sent	The number of DHCP messages that were sent by the DHCP server.

21-32 vrf (DHCP Pool)

This command is used to associate the address pool with a VRF name.

vrf *VRF-NAME*

no vrf *VRF-NAME*

Parameters

VRF-NAME	Specifies the name of the VRF to which the address pool is associated with.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

By default, the address pool is defined for the global routing domain. Associating a pool with a VRF allows overlapping addresses of other pools that are not on the same VRF. Only one pool can be associated with each VRF. If the address pool is associated with a VRF, the DHCP server will only assign an IP address from the address pool when the associated VRF matches the VRF of the DHCP request.

Example

This example shows how to associate the on-demand address pool with a VRF named pool1.

```
Switch# configure terminal
Switch(config)# ip dhcp pool pool1
Switch(config-dhcp-pool)# vrf pool1
Switch(config-dhcp-pool)#
```

22. DHCP Snooping Commands

22-1 ip dhcp snooping

This command is used to globally enable DHCP snooping. Use the **no** 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.

Command Default Level

Level: 12.

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)#
```

22-2 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 the 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 disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 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)#
```

22-3 ip dhcp snooping database

This command is used to configure the storing of DHCP snooping binding entries to the local flash or a remote site. Use the **no** 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 one of the following forms: • ftp://username:password@location:tcpport/filename • tftp://location/filename • flash:/filename Note: The flash option only includes the external memory (like CF/SD/USB storage).
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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to store the DHCP binding entry to local flash or remote server. Use the follow methods to store DHCP binding entries:

- **flash:** Store the entries to a file in local file system.
- **tftp:** Store the entries to remote site via TFTP.
- **ftp:** Store the entries to remote site via FTP.

Note: The flash only includes the external memory like CF/SD/USB storage.

Use this command to save the DHCP snooping binding database in the stack switch. The database is not saved in a stack member switch.

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)#
```

22-4 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

When you enter this command, the switch will clear the database statistics.

Example

This example shows how to clear the snooping database statistics.

```
Switch# clear ip dhcp snooping database statistics
Switch#
```

22-5 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	Specifies the MAC address to clear.
IP-ADDRESS	Specifies the IP address to clear.
vlan *VLAN-ID*	Specifies the VLAN ID to clear.
interface *INTERFACE-ID*	Specifies the interface to clear.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

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#
```

22-6 renew ip dhcp snooping database

This command is used to renew the DHCP binding database.

renew ip dhcp snooping database *URL*

Parameters

URL	Specifies load the bind entry database from the URL and add the entries to the DHCP snooping binding entry table.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Using this command will cause the system 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#
```

22-7 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 to add or delete.
vlan *VLAN-ID*	Specifies the VLAN of the entry to add or delete.
IP-ADDRESS	Specifies the IP address of the entry to add or deleted.
INTERFACE-ID	Specifies the interface (physical port and port channel) on which to add or delete a binding entry.
SECONDS	Specifies the interval after which bindings are no longer valid. This value must be between 60 and 4294967295 seconds.
MAC-ADDRESS	Specifies the MAC address of the entry to add or delete.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

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 eth3/0/10 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 eth3/0/10
expiry 100
Switch#
```

This example shows how to disable 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 eth3/0/10.

```
Switch# ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth3/0/10
Switch#
```

22-8 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 return 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.

Command Default Level

Level: 12.

Usage Guideline

This command is 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, DHCPNAK, or DHCPLEASEQUERY 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 3/0/3.

```
Switch# configure terminal
Switch(config)# interface eth3/0/3
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)#
```

22-9 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** command to reset the DHCP message entry limit.

ip dhcp snooping limit entries {*NUMBER* **| no-limit}**

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.
no-limit	Specifies no binding entry number limitation.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is 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 eth3/0/1 to 100.

```
Switch# configure terminal
Switch(config)# interface eth3/0/3
Switch(config-if)# ip dhcp snooping limit entries 100
Switch(config-if)#
```

22-10 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** command to reset the DHCP message rate limiting.

ip dhcp snooping limit rate {*VALUE* **| no-limit}**

no ip dhcp snooping limit rate

Parameters

rate *VALUE*	Specifies the number of DHCP messages that can be processed per second. The valid range is from 1 to 300.
no-limit	Specifies no limitation on the rate.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 3/0/3.

```
Switch# configure terminal
Switch(config)# interface eth3/0/3
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)#
```

22-11 ip dhcp snooping station-move deny

This command is used to disable the DHCP snooping station move state. Use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

When 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)#
```

22-12 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** 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.

Command Default Level

Level: 12.

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)#
```

22-13 ip dhcp snooping vlan

This command is used to enable DHCP snooping on a VLAN or a group of VLANs. Use the **no** 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 *VLAN-ID*	Specifies the VLAN to enable or disable the DHCP snooping function.
,	(Optional) Specifies a series of interfaces, or separate a range of

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

Default

By default, DHCP snooping is disabled on all VLANs.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 enable DHCP snooping on a range of VLANs.

```
Switch# configure terminal
Switch(config)# ip dhcp snooping vlan 10,15-18
Switch(config)#
```

22-14 show ip dhcp snooping

This command is used to display the DHCP snooping configuration.

show ip dhcp snooping

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 enabled
DHCP Snooping is enabled on VLANs:
10, 15-18
Verification of MAC address is disabled
Information option of allowed on un-trusted interface is disabled

Interface    Trusted    Rate Limit
------------ ---------- ------------
eth3/0/1        no      10
eth3/0/8        no      50
eth3/0/9        yes     no_limit

Switch#
```

22-15 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 *INTERFACE-ID*	(Optional) Specifies to display the binding entry based on the port ID.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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    eth3/0/5
00-01-02-00-00-05 10.1.1.11        1495           dhcp-snooping   100    eth3/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1.

```
Switch# show ip dhcp snooping binding 10.1.1.1

MAC Address       IP Address      Lease (seconds)   Type           VLAN   Interface
----------------- --------------- ----------------  -------------- ------ ----------
00-01-02-03-04-05 10.1.1.1        1500              dhcp-snooping  100    eth3/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.11 and MAC 00-01-02-00-00-05.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05

MAC Address         IP Address   Lease (seconds)     Type          VLAN   Interface
----------------- --------------- ------------------  ------------- ------ -----------
00-01-02-00-00-05 10.1.1.11      1495                dhcp-snooping 100    eth3/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1 and MAC 00-01-02-03-04-05 on VLAN 100.

```
Switch# show ip dhcp snooping binding 10.1.1.11 00-01-02-00-00-05 vlan 100

MAC Address         IP Address    Lease (seconds)   Type           VLAN   Interface
----------------- --------------- ----------------  -------------- ------ -----------
00-01-02-03-04-05 10.1.1.1        1500              dhcp-snooping  100    eth3/0/5

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    eth3/0/5
00-01-02-00-00-05 10.1.1.11       1495               dhcp-snooping  100    eth3/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries by interface eth3/0/5.

```
Switch# show ip dhcp snooping binding interface eth3/0/5

MAC Address         IP Address   Lease (seconds)   Type           VLAN   Interface
----------------- -------------- ----------------  -------------- ------ -----------
00-01-02-03-04-05 10.1.1.10      1500              dhcp-snooping  100    eth3/0/5
00-01-02-00-00-05 10.1.1.11      495               dhcp-snooping  100    eth3/0/5

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.

22-16 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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.

22-17 based-on hardware-address

This command is used to add or delete an entry of the DHCP server screen profile.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Parameters

CLIENT-HARDWARE-ADDRESS	(Optional) Specifies the MAC address of the client.

Default

None.

Command Mode

Configure DHCP Server Screen Mode.

Command Default Level

Level: 12.

Usage Guideline

If a binding entry is defined with the client's MAC address, then 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.

If a binding entry is defined without the client's MAC address, then the server message with the specified server IP address in the payload will be permitted. These binding entries restrict that only specific servers are allowed to offer DHCP server services.

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)#
```

22-18 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.

Command Default Level

Level: 12.

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#
```

22-19 dhcp-server-screen profile

This command is used to define a server screen profile and enter the server screen configure mode.

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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the DHCP server screen configuration 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)#
```

22-20 ip dhcp snooping server-screen

This command is used to enable or disable DHCP server screening.

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.

Command Default Level

Level: 12.

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 for port eth2/0/3.

```
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 eth2/0/3
switch(config-if)# ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
switch(config-if)#
```

22-21 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 the command to return to the default setting.

ip dhcp snooping server-screen log-buffer entries *NUMBER*

no ip dhcp snooping server-screen log-buffer entries

Parameters

NUMBER	(Optional) Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

22-22 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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#
```

23. DHCPv6 Client Commands

23-1 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command restarts the IPv6 DHCP client on the specified interface.

Example

This example shows how to restart the DHCPv6 client for interface VLAN 1.

```
Switch# clear ipv6 dhcp client vlan1
Switch#
```

23-2 ipv6 dhcp client pd

This command is used to enable the Dynamic Host Configuration Protocol (DHCP) IPv6 client process to request the prefix delegation through a specified interface. Use the **no** form of this command to disable the request.

ipv6 dhcp client pd *PREFIX-NAME* **[rapid-commit]**

no ipv6 dhcp client pd

Parameters

PREFIX-NAME	Specifies the IPv6 general prefix name with a maximum of 32 characters.
rapid-commit	Specifies to proceed with two-message exchange for prefix 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the prefix delegation request through an interface. The interface being configured will be in DHCP client mode. The prefix acquired from the server will be stored in the IPv6 general prefix pool represented by the general prefix name of the command, which will be in turn used in configuration of IPv6 addresses. Only one general prefix name can be specified for DHCPv6 PD on an interface. However, a general prefix name can be specified for DHCPv6 PD on multiple interfaces.

If the rapid commit keyword is specified for the command, the rapid commit option will be included in the solicit message to request for the two-message exchange for prefix delegation.

When the client receives advertisement from multiple servers, the client will take the server with best preference value. The client can accept multiple prefixes delegated from a server.

The DHCP for IPv6 client, server and relay functions are mutually exclusive on an interface.

Example

This example shows how to configure an IPv6 address based on the general prefix “dhcp-prefix” on VLAN 2 and enables DHCPv6 prefix delegation on VLAN 1 with “dhcp-prefix” as the general prefix name and with the rapid commit option.

```
Switch# configure terminal
Switch(config)# interface vlan2
Switch(config-if)# ipv6 address dhcp-prefix 0:0:0:7272::72/64
Switch(config-if)# exit
Switch(config)# interface vlan1
Switch(config-if)# ipv6 dhcp client pd dhcp-prefix rapid-commit
Switch(config-if)#
```

23-3 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	Specifies the VLAN interface to display the DHCPv6 related settings.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the device's DHCPv6 DUID or 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 0001000111A8040D001FC6D1D47B.

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 liftime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```

24. DHCPv6 Guard Commands

24-1 ipv6 dhcp guard policy

This command is used to create or modify a DHCPv6 guard policy. This command will enter into the DHCPv6 guard configuration mode. Use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create or modify the DHCPv6 guard policy. This command will enter into the DHCPv6 guard 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)# device-role server
Switch(config-dhcp-guard)# match ipv6 access-list acl1
Switch(config-dhcp-guard)#
```

24-2 device-role

This command is used to specify the role of the attached device.

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.

Command Default Level

Level: 12.

Usage Guideline

The command is used 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's role as the server.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp guard policy dhcpguard1
Switch(config-dhcp-guard)# device-role server
Switch(config-dhcp-guard)#
```

24-3 match ipv6 access-list

This command is used to verify the sender's IPv6 address in server messages. Use the **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

24-4 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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 interface eth1/0/3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

24-5 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the policy name is specified, only the specified policy information is displayed. If the policy name is not specified, information is displayed for all policies.

Example

This example shows how to displayed for 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.

25. DHCPv6 Relay Commands

25-1 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 the command to remove a relay destination.

ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

no ipv6 dhcp relay destination *IPV6-ADDRESS*

Parameters

IPV6-ADDRESS	Specifies the DHCPv6 relay destination address.
INTERFACE-ID	Specifies the output interface for the relay destination.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To enable the DHCPv6 relay function on an interface, use the **ipv6 dhcp relay destination** command to configure the relay destination address on an interface. Use the **no ipv6 dhcp relay destination** command to remove the relay address. 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)#
```

25-2 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 *SUB-TYPE-NAME*

no ipv6 dhcp relay remote-id format

Parameters

SUB-TYPE-NAME	Specifies the string that identifies the sub-type for the remote ID to be configured.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used 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)#
```

25-3 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 the 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.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable 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)#
```

25-4 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 the command to restore 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the global policy for packets that already have Option 37. If the **drop** policy is selected, 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** policy is selected, the switch doesn't 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)#
```

25-5 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

25-6 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 ID to display.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the device's DHCPv6 DUID or use the **show ipv6 dhcp interface** command to display DHCPv6 related settings and information for the specified VLAN interface. If the interface ID is not specified, all interfaces that are enabled for 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#
```

25-7 show ipv6 dhcp relay information option

This command is used to display settings of the DHCPv6 relay information options.

show ipv6 dhcp relay information option

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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#
```

26. DHCPv6 Server Commands

26-1 address prefix

This command is used to specify an address prefix for address assignment. Use the **no** form of this command to remove the address prefix.

address prefix *IPV6-PREFIXIPREFIX-LENGTH* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

no address prefix

Parameters

IPV6-PREFIX	Specifies the IPv6 address prefix to assign to the client.
PREFIX-LENGTH	Specifies the length of the IPv6 address prefix.
lifetime *VALID-LIFETIME*	(Optional) Specifies the valid lifetime of the address prefix in seconds. The valid lifetime value should be greater than preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime value is 2592000 seconds (30 days).
PREFERRED-LIFETIME	(Optional) Specifies the preferred lifetime of the address prefix in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime value is not specified, the default lifetime value is 604800 seconds (7 days)

Default

None.

Command Mode

DHCPv6 Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure an address prefix in an IPv6 DHCP pool configuration. Only one address prefix can be configured for a DHCPv6 pool. The latter issued command will overwrite the previous.

When the server receives a request from a client, the server will check the IPv6 DHCP pool associated with the received interface. If static binding address entries are defined to assign the address for the request client, that static binding address will be assigned. Otherwise, the server will assign the address from the address prefix specified for the IPv6 DHCP pool.

Example

This example shows how to configure the address prefix 2001:0DB8::0/64 to the IPv6 DHCP pool “pool1”.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#
```

26-2 address-assignment

This command is used to specify an address to be assigned to a specified client. Use the **no** form of this command to remove the static binding address.

address-assignment *IPV6-ADDRESS CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

no address-assignment *IPV6-ADDRESS*

Parameters

IPV6-ADDRESS	Specifies the IPv6 address to assign to the specific client.
CLIENT-DUID	Specifies the DHCP unique identifier (DUID) of the client to get the address.
iaid *IAID*	(Optional) Specifies an identity association identifier (IAID). The IAID here uniquely identifies a collection of non-temporary addresses (IANA) assigned on the client.
lifetime *VALID-LIFETIME*	(Optional) Specifies the valid lifetime of the address in seconds. The valid lifetime should be greater than the preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime is the pool's valid lifetime.
PREFERRED-LIFETIME	(Optional) Specifies the preferred lifetime of the address in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default preferred lifetime is the pool's preferred lifetime.

Default

None.

Command Mode

DHCPv6 Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to configure a static binding address entry to specify the address to be assigned to specific client.

When the server receives a request from a client, the server will check the IPv6 DHCP pool associated with the received interface. If the request message includes the IANA option and there are free static entries that are configured with IAID and match both the DUID and IAID of the message, then the match entry will be assigned. If there is no match entry, then if there are free static entries without IAID specified and match the DUID of the message, then the match entry are replied.

If there are no match entries, the client will be assigned with the address from the address prefix specified in the IPv6 DHCP pool.

Example

This example shows how to configure a static binding address entry in an IPv6 DHCP pool named "pool1" and associates the IPv6 DHCP pool with VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(dhcpv6-config)# address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan100
```

```
Switch(dhcpv6-config)# ipv6 dhcp server pool1
Switch(dhcpv6-config)#
```

This example shows how to configure a static binding address entry in an IPv6 DHCP pool named “pool2” with IAID option and associates the IPv6 DHCP pool with VLAN 200.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool2
Switch(dhcpv6-config)# address-assignment 2001:AAB8::2:2 00030001050611223344 iaid
0x123
Switch(dhcpv6-config)# exit
Switch(config)# interface vlan200
Switch(config-if)# ipv6 dhcp server pool2
Switch(config-if)#
```

26-3 clear ipv6 dhcp binding

This command is used to delete the DHCPv6 server binding entries.

clear ipv6 dhcp binding {all | *IPV6-PREFIX***}**

Parameters

all	Specifies to clear all binding entries.
IPV6-PREFIX	Specifies the binding entry by prefix to be cleared.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to clear the DHCPv6 server binding entries. If an IPv6 prefix is specified for the command, the binding entry corresponding to the specified client is cleared. Otherwise, all binding entries will be cleared. The IPv6 prefix being freed will be returned to the pool it is originally allocated.

Example

This example shows how to clear all the binding entries in the DHCPv6 server binding table.

```
Switch# clear ipv6 dhcp binding all
Switch#
```

26-4 domain-name

This command is used to configure a domain name to be assigned to the requesting DHCPv6 client. Use the **no** form of this command to remove the domain name specification.

domain-name *DOMAIN-NAME*

no domain-name *DOMAIN-NAME*

Parameters

DOMAIN-NAME	Specifies the domain name.

Default

None.

Command Mode

DHCPv6 Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the domain name to be assigned to the requesting DHCPv6 client. Only one domain name can be specified.

Example

This example shows how to configure the domain name in a DHCPv6 server pool named “pool1”.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# domain-name v6domain
Switch(config-dhcp)#
```

26-5 dns-server

This command is used to configure the DNS IPv6 server list to be assigned to the requesting IPv6 client. Use the **no** form of this command to remove a DNS server from the server list.

dns-server *IPV6-ADDRESS*

no dns-server *IPV6-ADDRESS*

Parameters

IPV6-ADDRESS	Specifies the IPv6 address of the DNS server.

Default

None.

Command Mode

DHCPv6 Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the DNS IPv6 server address to be assigned to the requesting DHCPv6 client. Multiple server addresses can be configured by setting this command multiple times.

Example

This example shows how to configure a DNS IPv6 server in the DHCPv6 server pool named “pool1”.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# dns-server 2001:0DB8:3000:3000::42
Switch(config-dhcp)#
```

26-6 ipv6 dhcp excluded-address

This command is used to specify IPv6 addresses that a DHCPv6 server should not assign to DHCP clients. Use the **no** form of the command to remove the excluded IPv6 address.

ipv6 dhcp excluded-address *LOW-ADDRESS* **[***HIGH-ADDRESS***]**

no ipv6 dhcp excluded-address *LOW-ADDRESS* **[***HIGH-ADDRESS***]**

Parameters

LOW-ADDRESS	Specifies the excluded IPv6 address or first IPv6 address in an excluded address range.
HIGH-ADDRESS	(Optional) Specifies the last IPv6 address in the excluded address range.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The DHCPv6 server assumes that all addresses (excluding the switch’s IPv6 address) can be assigned to clients. Use this command to exclude a single IPv6 address or a range of IPv6 addresses. The excluded addresses are only applied to the pool(s) for address assignment.

Example

This example shows how to configure the IPv6 address 3004:DB8::1:10 to the excluded address.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp excluded-address 3004:DB8::1:10
Switch(config)#
```

26-7 ipv6 dhcp pool

This command is used to enter the DHCP pool configuration mode and configure the IPv6 DHCP pool. Use the **no** form of the command to remove the IPv6 DHCP pool.

ipv6 dhcp pool *POOL-NAME*

no ipv6 dhcp pool *POOL-NAME*

Parameters

POOL-NAME	Specifies the name for the address pool. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the IPv6 DHCP pool configuration mode and configure the IPv6 DHCP pool. Use the **ipv6 dhcp server** command to enable the DHCP IPv6 server service on an interface and specify the IPv6 DHCP pool used to service the DHCP request received on the interface.

Example

This example shows how to configure the address pool named “pool1”.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)#
```

26-8 ipv6 dhcp server

This command is used to enable the DHCP IPv6 server service on an interface. Use the **no** form of this command to disable the DHCP Ipv6 server service on an interface.

ipv6 dhcp server *POOL-NAME* **[rapid-commit]**

no ipv6 dhcp server

Parameters

POOL-NAME	Specifies the name of the IPv6 DHCP pool used to serve the request received on the interface.
rapid-commit	(Optional) Specifies to allow the proceeding of two-message exchange. By default, two-message exchange is not allowed.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables DHCP for IPv6 server service on a specified interface.

An IPv6 DHCP pool can be associated with multiple interfaces. The pool must be configured before it can be associated. Only one IPv6 DHCP pool can be associated with an interface. The DHCP for the IPv6 client, server, and relay functions are mutually exclusive on an interface.

If the command is configured with the **rapid-commit** option, the server will proceed the two-message exchange for prefix delegation and other configuration if the client has included a rapid commit option in the solicit message.

Example

This example shows how to create the DHCP pool “pool1”, enable the DHCP IPv6 server service on the interface VLAN 100 using the DHCP pool “pool1” to delegate the prefixes.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# exit
Switch(config)# interface vlan100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26-9 ipv6 local pool

This command is used to configure a local IPv6 prefix pool. Use the **no** form to remove the pool.

ipv6 local pool *POOL-NAME IPV6-PREFIXIPREFIX-LENGTH ASSIGNED-LENGTH*

no ipv6 local pool *POOL-NAME*

Parameters

POOL-NAME	Specifies the name of the local IPv6 prefix pool with a maximum of 32 characters.
IPV6-PREFIX	Specifies the IPv6 prefix address of the local pool.
PREFIX-LENGTH	Specifies the IPv6 prefix length of the local pool.
ASSIGNED-LENGTH	Specifies the prefix length to delegate to the user from the pool. The value of the assigned length cannot be less than the value of the prefix length.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A local IPv6 prefix pool defines a block of prefixes. Define the pool with overlay prefixes with other pools. To modify the prefix for the local pool, remove the local pool first and re-create the pool. All of the prefixes that are already allocated will be freed.

Example

This example shows how to create a local IPv6 prefix pool named “prefix-pool” and use the local pool in the DHCP pool “pool1”.

```
Switch# configure terminal
Switch(config)# ipv6 local pool prefix-pool 3004:DB8::/48 64
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#
```

26-10 prefix-delegation

This command is used to specify a prefix to be delegated to the specified client. Use the **no** form of this command to remove the static binding prefix.

prefix-delegation *IPV6-PREFIXIPREFIX-LENGTH CLIENT-DUID* **[iaid** *IAID***] [lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

no prefix-delegation *IPV6-PREFIXIPREFIX-LENGTH*

Parameters

IPV6-PREFIX	Specifies the IPv6 prefix to delegate to the specific client.
PREFIX-LENGTH	Specifies the length of the IPv6 prefix.
CLIENT-DUID	Specifies the DHCP unique identifier (DUID) of the client to get the delegation.
iaid *IAID*	(Optional) Specifies the identity association identifier (IAID). An IAID uniquely identifies a collection of prefixes assigned to the requesting router.
lifetime *VALID-LIFETIME*	(Optional) Specifies the valid lifetime of the prefix in seconds. The valid lifetime should be greater than preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime is 2592000 seconds (30 days).
PREFERRED-LIFETIME	(Optional) Specifies the preferred lifetime of the prefix in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default preferred lifetime is 604800 seconds (7 days)

Default

None.

Command Mode

DHCPv6 Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure a static binding prefix entry to specify the prefix to be dedicatedly delegated to specific client. Multiple static binding prefix entry can be defined for a client, or an IAPD on a client.

When the server receives a request from a client, the server will check the IPv6 DHCP pool associated with the received interface. If the request message includes the IAPD option and there are free static entries that are configured with IAID and match both the DUID and IAID of the message, then all the match entries will be delegated. If there are no match entries, then if there are free static entries without IAID specified and match the DUID of the message, then the match entries are replied. If the request message has no IAID option, t then if there are free static entries without IAID specified and match the DUID of the message, then the match entries are replied.

If there are no match entries, the client will be delegated the prefix from the local IPv6 prefix pool specified in the IPv6 DHCP pool.

Example

This example shows how to configure a static binding prefix entry in a IPv6 DHCP pool named “pool1” and associates the IPv6 DHCP pool with VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation 2001:0DB8::/64 000300010506BBCCDDEE
Switch(config-dhcp)# exit
Switch(config)# interface vlan100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26-11 prefix-delegation pool

This command is used to specify a local IPv6 prefix pool from which prefixes can be delegated. Use the **no** form of the command to move a local IPv6 prefix pool.

prefix-delegation pool *POOL-NAME* **[lifetime** *VALID-LIFETIME PREFERRED-LIFETIME***]**

no prefix-delegation pool *POOL-NAME*

Parameters

POOL-NAME	Specifies the name of a local IPv6 prefix pool.
lifetime *VALID-LIFETIME*	(Optional) Specifies the valid lifetime of the prefix in seconds. The valid lifetime should be greater than preferred lifetime. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default valid lifetime is 2592000 seconds (30 days).
lifetime *PREFERRED-LIFETIME*	(Optional) Specifies the preferred lifetime of the prefix in seconds. This value must be between 60 and 4294967295, or infinite. If the lifetime is not specified, the default preferred lifetime is 604800 seconds (7 days)

Default

None.

Command Mode

DHCPv6 Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify a local IPv6 prefix pool in a IPv6 DHCP pool to delegate the prefix for clients serviced by the DHCP pool. Only one local IPv6 prefix pool can be specified in an IPv6 DHCP pool.

When the server receives a request from a client, the server will check the IPv6 DHCP pool associated with the received interface. If static binding prefix entries are defined to delegate the prefix for the request client, the static binding prefix will be delegated. Otherwise, the server will delegate the prefix from the local IPv6 prefix pool specified for the IPv6 DHCP pool.

Example

This example shows how to configure a local IPv6 prefix pool named “client-prefix”, specify the pool in an IPv6 DHCP pool named “pool1” and associate the IPv6 DHCP pool with VLAN 100.

```
Switch# configure terminal
Switch(config)# ipv6 local pool client-prefix 3004:DB8::/48 64
Switch(config)# ipv6 dhcp pool pool1
Switch(config-dhcp)# prefix-delegation pool client-prefix lifetime 300 200
Switch(config-dhcp)# exit
Switch(config)# interface vlan100
Switch(config-if)# ipv6 dhcp server pool1
Switch(config-if)#
```

26-12 service ipv6 dhcp

This command is used to enable the IPv6 DHCP server and relay service on the switch. Use the **no** form of this command to disable the IPv6 DHCP server and relay service.

service pv6 dhcp

no service ipv6 dhcp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to globally enable the IPv6 DHCP server and relay service on the switch. The configuration changes of the DHCPv6 server cannot take effect in real-time, disable and enable the DHCPv6 server to make the new configuration take effect.

Example

This example shows how to enable the IPv6 DHCP server and relay service.

```
Switch# configure terminal
Switch(config)# service ipv6 dhcp
Switch(config)#
```

26-13 show ipv6 dhcp

This command is used to display the DHCPv6 related setting for interfaces.

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

Parameters

INTERFACE-ID	(Optional) Specifies the VLAN interface to display the DHCPv6 related setting.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the device's DHCPv6 DUID or use the **show ipv6 dhcp interface** command to display the DHCPv6 related settings for interfaces. If the interface ID is not specified, all interfaces that are enabled with the DHCPv6 function will be displayed.

Example

This example shows how to display the DHCPv6 information for 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#
```

This example shows how to display the DHCPv6 client for interface VLAN 1, when VLAN 1 is DHCPv6 server enabled.

```
Switch# show ipv6 dhcp interface vlan1

Vlan1 is in server mode
IPv6 DHCP pool is pool1
Rapid-Commit is disabled

Switch#
```

26-14 show ipv6 dhcp binding

This command is used to display the IPv6 prefix binding entry.

show ipv6 dhcp binding [*IPV6-PREFIX***]**

Parameters

IPV6-PREFIX	(Option) Specifies the binding entry to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays all DHCPv6 client prefix bindings from the binding table if the IPV6 prefix parameter is not given. If the IPV6 prefix parameter is given, it only displays the specific client prefix binding for the prefix.

Example

This example shows how to display the IPv6 prefix binding entry.

```
Switch# show ipv6 dhcp binding

Client DUID : 00010002
Prefix: 2004::/64
            preferred lifetime 60, valid lifetime 120

Client DUID : 00010003
address: 2005::1/64
            preferred lifetime 60, valid lifetime 120

Total Entries: 2

Switch#
```

26-15 show ipv6 dhcp pool

This command is used to display the DHCPv6 server configuration pool information.

show ipv6 dhcp pool [*POOL-NAME***]**

Parameters

POOL-NAME	(Optional) Specifies the IPv6 DHCP pool to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays all DHCPv6 server configuration pool information if the pool name parameter is not specified. Otherwise, it only displays the pool information for the specified pool name.

Example

This example shows how to display the DHCPv6 pool information.

```
Switch# show ipv6 dhcp pool

DHCPv6 pool: abc
        Static bindings:
           Binding for client 00030006000000001111
             IA PD: IA ID not specified
             Prefix: 2000:0:200::/48
             preferred lifetime 1000, valid lifetime 2000
        Prefix delegation pool: aaa
              preferred lifetime 1000, valid lifetime 2000
        DNS server:
        Domain name:
        Active clients: 0

DHCPv6 pool: test
        Static bindings:
           Binding for client 00030006000000001111
            IA NA: IA ID not specified
              Address: 2013::2013
               preferred lifetime 2000, valid lifetime 3000
           Binding for client 00030006000000001112
            IA NA: IA ID not specified
              Address: 2013::2023
               preferred lifetime 150, valid lifetime 200
        Address prefix: 2013::/64
              preferred lifetime 2000, valid lifetime 3000
        DNS server:
        Domain name:
        Active clients: 0

Switch#
```

Display Parameters

DHCPv6 pool	The name of the pool.
Binding for client 000300010002FCA5C01C	Indicates a static binding for the client with the DUID 000300010002FCA5C01C.
IAPD	The collection of prefixes assigned to a client.
IAID	The identity association identifier for this IAPD.
Prefix	The prefixes to be delegated.

preferred lifetime, valid lifetime	The preferred lifetime and valid lifetime assigned to this prefix for client.
DNS server	The DNS server address list.
Domain name	The configured DNS domain list.
Active clients	The total number of active clients.

26-16 show ipv6 excluded-address

This command is used to display the IPv6 excluded address configuration information.

show ipv6 excluded-address

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the excluded address range which cannot be assigned to the client.

Example

This example shows how to displays the configured exclude addresses.

```
Switch# show ipv6 excluded-address

IPv6 excluded address:
1.3004:DB8::1:10
2.3004:DBB::1:100 – 3004:DBB::1:105

Total Entries: 2

Switch#
```

26-17 show ipv6 local pool

This command is used to display the local IPv6 prefix pool configuration information.

show ipv6 local pool [*POOL-NAME***]**

Parameters

POOL-NAME	(Optional) Specifies the local IPv6 prefix pool to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the settings for a specific local IPv6 prefix pool or the setting for all prefix if the pool name parameter is not specified.

Example

This example shows how to display the local pool information without the pool name specified.

```
Switch# show ipv6 local pool

Pool         Prefix                                        Free In use
------------ --------------------------------------------- ---- ------
aaa          2000::/32                                     65536 0
------------ --------------------------------------------- ---- ------

Total Entries: 2

Switch#
```

This example shows how to display the information for local pool called “PP1”.

```
Switch# show ipv6 local pool PP1

Prefix is 2003::/46 assign /62 prefix
1 entries in use, 65535 available, 0 rejected
User                        Prefix          Interface
000300010002FCA5C01C    2003::/64       Vlan1

Switch#
```

27. Digital Diagnostics Monitoring (DDM) Commands

27-1 show interfaces transceiver

This command is used to display the current SFP module operating parameters.

show interfaces [*INTERFACE-ID* **[,|-] transceiver [detail]**

Parameters

INTERFACE-ID **[,|-]**	(Optional) Specifies multiple interfaces for transceiver monitoring status display. If no interface ID is specified, transceiver monitoring statuses on all valid interfaces are displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the current SFP module operating transceiver monitoring parameters values for specified ports.

Example

This example shows how to display current operating parameters for all ports valid for transceiver monitoring.

```
Switch# show interfaces transceiver

++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts#

         Temperature  Voltage      Bias Current TX Power     RX Power
port     (Celsius)    (V)          (mA)         (mW)         (mW)
-------- ------------ ------------ ------------ ------------ ------------
eth2/0/23     30.090     3.353      16.794(++)    0.258       0.000(--)
eth3/0/25     29.316     3.302       5.326        0.529       0.506
eth3/0/26     31.617     3.297       5.170        0.527       0.504

Total Entries: 3

Switch#
```

This example shows how to display detailed transceiver monitoring information for all ports which are valid for transceiver monitoring.

```
Switch# show interfaces transceiver detail
```

```
++ : high alarm, +  : high warning, -  : low warning, -- : low alarm
mA: milliamperes, mW: milliwatts
A: The threshold is administratively configured.

eth2/0/3
Transceiver Monitoring is enabled
Transceiver Monitoring shutdown action：Alarm

                  Current     High-Alarm  High-Warning Low-Warning Low-Alarm
Temperature(C)    30.090      75.000(A)   70.000       0.000       -5.000
Voltage (v)        3.353       3.630       3.465       3.135        2.970
Bias Current(mA)  16.794(++)  10.500       9.000       2.500        2.000
TX Power (mW)      0.258       1.413       0.708       0.186        0.074
RX Power (mW)      0.000(--)   1.585       0.794       0.102        0.041

Switch#
```

27-2 transceiver-monitoring action shutdown

This command is used to shut down a port from an alarm or a warning of an abnormal status.

Use the **no** form of the command to disable the shutdown action.

transceiver-monitoring action shutdown { alarm | warning}

no transceiver-monitoring action shutdown

Parameters

alarm	Specifies to shut down a port when alarm events occur.
warning	Specifies to shut down a port when warning events occur.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port interface configuration.

The configuration can select to shut down a port on an alarm event or warning event or not to shut down on either of them. When the monitoring function is enabled, an alarm event occurs when the parameters, being monitored, go higher than the high alarm threshold or go lower than the low alarm threshold. A warning event occurs when the parameters being monitored go higher than the high warning threshold or go lower than the low warning threshold.

The port shutdown feature is controlled by the Error Disable module without a recover timer. Users can manually recover the port by using the **shutdown** command and then the **no shutdown** command.

Example

This example shows how to configure the shutdown interface eth3/0/1 when an alarm event is detected.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# transceiver-monitoring action shutdown alarm#
Switch(config-if)#
```

27-3 transceiver-monitoring bias-current

This command is used to configure the thresholds of the bias current for a specified port.

Use the **no** form of the command to remove the configuration.

transceiver-monitoring bias-current *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*

no transceiver-monitoring bias-current *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

INTERFACE-ID	Specifies the interface to modify.
high	Specifies the high threshold, when the operating parameter rises above this value. It indicates an abnormal status.
low	Specifies the low threshold, when the operating parameter falls below this value, It indicates an abnormal status.
alarm	Specifies the threshold for high alarm or low alarm conditions.
warning	Specifies the threshold for high warning or low warning conditions.
VALUE	Specifies the value of the threshold. This value must be betwee 0 and 131 mA.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This configuration is only suitable for SFP/SFP+ port interfaces with optical modules with transceiver-monitoring.

This command configures the bias-current thresholds on the specified ports. The value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then rewritten into the SFP module.

If the SFP module being configured does not support the threshold change, the user-configured threshold is stored in the system and the displayed value will be the user-configured threshold. If no user-configured threshold exists, the displayed value will always reflect the factory preset value defined by vendors.

The **no** form of this command has the effect to clear the configured threshold stored in the system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values on newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the bias current high warning threshold as 10.237 on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring bias-current eth3/0/1 high warning 10.237

WARNING: A closest value 10.238 is chosen according to the transceiver-monitoring
precision definition

Switch(config)#
```

27-4 transceiver-monitoring enable

This command is used to enable the optical transceiver monitoring function for an SFP port. Use the **no** form of the command to disable optical transceiver monitoring.

transceiver-monitoring enable

no transceiver-monitoring enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for the physical port interface configuration.

A user can use this command to enable or disable optical transceiver monitoring functions for an SFP port. When the monitoring function is enabled, an alarm event occurs when the parameters being monitored go higher than the high alarm threshold or go lower than the low alarm threshold. A warning event occurs when the parameters being monitored go higher than the high warning threshold or go lower than the low warning threshold.

When an SFP with transceiver monitoring capability is plugged into a port but the transceiver monitoring function of the port is disabled, the system will not detect the SFP's abnormal status but the user can still check the current status by showing the interface transceiver command.

Example

This example shows how to enable transceiver monitoring on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# transceiver-monitoring enable
Switch(config-if)#
```

27-5 transceiver-monitoring rx-power

This command is used to configure the thresholds of the input power for the specified port. Use the **no** form of the command to remove the configuration.

transceiver-monitoring rx-power *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **| dbm** *VALUE***}**

no transceiver-monitoring rx-power *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

INTERFACE ID	Specifies the interface to modify.
high	Specifies that when the operating parameter rises above the highest threshold, it indicates an abnormal status
low	Specifies that when the operating parameter falls below the low threshold this value, it indicates an abnormal status.
alarm	Specifies to configure the high and low threshold value condition.
warning	Specifies to configure the high and low warning threshold conditions.
mwatt *VALUE*	Specifies the power threshold value in milliwatts. This value must be between 0 and 6.5535.
dbm *VALUE*	Specifies the power threshold value in dBm. This value must be between -40 and 8.1647.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only SFP/SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.

This command configures the RX power thresholds on the specified port. This value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP module.

If the SFP module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the RX power low warning threshold as 0.135 mW on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring rx-power eth3/0/1 low warning mwatt 0.135

WARNING: A closest value 0.135 is chosen according to the transceiver-monitoring
precision definition.

Switch(config)#
```

27-6 transceiver-monitoring temperature

This command is used to configure the temperature thresholds for the specified port. Use the **no** form of the command to remove the configuration.

transceiver-monitoring temperature *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*

no transceiver-monitoring temperature *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

INTERFACE ID	Specifies the interface to modify.
high	Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status.
low	Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status.
alarm	Specifies to configure the high and low threshold value condition.
warning	Specifies to configure the high and low warning threshold conditions.
VALUE	Specifies the threshold value. This value must be between -128 and 127.996 °C.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only SFP/SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.

This command configures the RX power thresholds on the specified port. This value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP module.

If the SFP module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the temperature high alarm threshold as 127.994 on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring temperature eth3/0/1 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring
precision definition
```

```
Switch(config)#
```

27-7 transceiver-monitoring tx-power

This command is used to configure the output power threshold for the specified port. Use the **no** form of the command to remove the configuration.

transceiver-monitoring tx-power *INTERFACE-ID* **{high | low} {alarm | warning} {mwatt** *VALUE* **| dbm** *VALUE***}**

no transceiver-monitoring tx-power *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

high	Specifies the interface to modify.
low	Specifies that when the operating parameter rises above this high threshold value, it indicates an abnormal status.
alarm	Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status.
warning	Specifies to configure the high and low warning threshold conditions.
mwatt *VALUE*	Specifies the power threshold value in milliwatts. This value must be between 0 and 6.5535.
dbm *VALUE*	Specifies the power threshold value in dBm. This value must be between -40 and 8.1647.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only SFP/SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.

This command configures the TX power thresholds on the specified port. This value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP module.

If the SFP module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the TX power low warning threshold to 0.181 mW on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring tx-power eth3/0/1 low warning mwatt 0.181

WARNING: The closest value of 0.181 is chosen according to the transceiver-monitoring
precision definition

Switch(config)#
```

27-8 transceiver-monitoring voltage

This command is used to configure the threshold voltage of the specified port. Use the **no** form of the command to remove the configuration.

transceiver-monitoring voltage *INTERFACE-ID* **{high | low} {alarm | warning}** *VALUE*

no transceiver-monitoring voltage *INTERFACE-ID* **{high | low} {alarm | warning}**

Parameters

INTERFACE-ID	Specifies the interface to modify.
high	Specifies that when the operating parameter rises above the highest threshold, it indicates an abnormal status.
low	Specifies that when the operating parameter falls below this low threshold value, it indicates an abnormal status.
alarm	Specifies to configure the high and low threshold value condition.
warning	Specifies to configure the high and low warning threshold conditions.
VALUE	Specifies the threshold value. This value must be between 0 and 6.5535 Volt.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only SFP/SFP+ port interfaces with optical modules, with transceiver monitoring capability, are valid for this configuration.

This command configures the voltage thresholds on the specified port. The value will be stored both in the system and in the SFP/SFP+ transceivers and be converted to the 16-bit format and then written into the SFP module.

If the SFP module configured does not support the threshold change, the user-configured threshold is just stored in the system and the displayed value will be the user-configured threshold. If there is no user-configured threshold, the displayed value will always reflect the factory preset value defined by the vendor.

The **no** form of this command has the effect to clear the configured threshold stored in system. It does not change the threshold stored in the SFP/SFP+ transceivers. Use the **no** form of the command to prevent threshold values in newly inserted SFP/SFP+ transceivers from being altered.

Example

This example shows how to configure the low alarm voltage threshold as 0.005 on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring voltage eth3/0/1 low alarm 0.005

WARNING: A closer value 0.005 is chosen according to the transceiver-monitoring
precision definition

Switch(config)#
```

28. Distance Vector Multicast Routing Protocol (DVMRP) Commands

28-1 ip dvmrp

This command is used to enable DVMRP on the current interface. Use the **no** form to disable DVMRP on the interface.

ip dvmrp

no ip dvmrp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The interface would start to run (or stop) the DVMRP protocol on the interface. Before enable the DVMRP function on an interface, the user should enable IP multicast routing by using the **ip multicast-routing** command in the global configuration mode. At most one multicast routing protocol can be enabled on one interface. Make sure no other multicast routing protocol is enabled before enabling DVMRP otherwise; an error message will be shown.

Example

This example shows how to enable the DVMRP protocol on the interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip dvmrp
```

28-2 ip dvmrp metric

This command is used to configure the metric associated with the route for Distance Vector Multicast Routing Protocol (DVMRP) reports. Use the **no** form of the command to return to the default value.

ip dvmrp metric *METRIC*

no ip dvmrp metric

Parameters

METRIC	Specifies the metric value. This value must be between 1 and 32. A

	value of 32 means infinity (unreachable).

Default

The default metric value is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

For each source network reported, a route metric is associated with the route being reported. The metric is the sum of the interface metrics between the router originating the report and the source network. For DVMRP, the metric with 32 means infinity (unreachable). This limits the breadth across the whole DVMRP network and is necessary to place an upper bound on the convergence time of the protocol.

Example

This example shows how to change the metric value to 2 of an interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip dvmrp metric 2
```

28-3 ip dvmrp neighbor-timeout

This command is used to configure the DVMRP neighbor lifetime value. Use the **no** form of the command to return to the default value.

ip dvmrp neighbor-timeout *SECONDS*

no ip dvmrp neighbor-timeout

Parameters

SECONDS	Specifies the neighbor lifetime value. It can be a value from 1 to 65535 seconds.

Default

By default, this value is 35 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the router has not received a probe message from a neighbor after the neighbor timeout interval, the neighbor is supposed to be down.

Example

This example shows how to configure the neighbor expiry time to 60 seconds for an interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip dvmrp neighbor-timeout 60
```

28-4 ip dvmrp probe-time

This command is used to configure the DVMRP probe interval. Use the **no** form of the command to return to the default value.

ip dvmrp probe-time *SECONDS*

no ip dvmrp probe-time

Parameters

SECONDS	Specifies the DVMRP probe interval value. It can be a value from 1 to 65535 seconds.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the interval time that the DVMRP router uses to send DVMRP Probe messages.

Example

This example shows how to change the probe time to 20 seconds of an interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip dvmrp probe-time 20
```

28-5 show ip dvmrp interface

This command is used to display DVMRP configuration information on an interface.

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

Parameters

INTERFACE-ID	(Optional) Specifies a single interface, a range of interfaces, separated by a hyphen, or a series of interfaces separated by a comma. Only the VLAN interface is allowed for this command.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays Distance Vector Multicast Routing Protocol (DVMRP) information on interfaces on which DVMRP is active. You can use the **show running-config** to further check the DVMRP configuration, if the interface is not displayed. If no interface is specified, all DVMRP active interfaces will be displayed.

Example

This example shows how to display DVMRP configure information for interface ‘vlan1000’.

```
Switch# show ip dvmrp interface vlan1000

NT = Neighbor Timeout
Interface  Address          NT   Probe    Metric  Generation ID  State
---------  ---------------- ----  -----  ------  -------------   ------
vlan1000   10.0.0.254      35      10    1       1234567890     Enabled

Total Entries: 1

Switch#
```

28-6 show ip dvmrp neighbor

This command is used to display DVMRP neighbor information.

show ip dvmrp neighbor [*INTERFACE-ID* **|** *IP-ADDRESS***]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID.
IP-ADDRESS	(Optional) Specifies the IP address of the neighbor.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display DVMRP neighbor information. If neither the interface ID nor the IP address is specified, information of all neighbors will be displayed

Example

This example shows how to display neighbor information.

```
Switch# show ip dvmrp neighbor

Interface        Neighbor Address  Generation ID  ExpTime
---------------  ----------------  -------------  -----------
vlan1            10.10.10.11       35ef6d         0DT00H00M29S

Total Entries: 1

Switch#
```

Display Parameters

Interface	The interface referred to the routing interface and it is mapped to a VLAN interface.
Neighbor Address	Once a system has received a probe from a neighbor, that contains the system's address in the neighbor list, the system has established a two-way neighbor adjacency with this router.
Generation ID	If a DVMRP router was restarted, it will not be aware of any previous prunes that it had sent or received. In order for the neighbor to detect that the router has restarted, a non-decreasing number is placed in the periodic probe message called the generation ID. When a change in the generation ID is detected, any prune information received from the router is no longer valid and should be flushed.
ExpTime	The neighbor timeout interval should be set at 35 seconds. This allows fairly early detection of a lost neighbor yet provides tolerance for busy multicast routers. These values must be coordinated between all DVMRP routers on a physical network segment. The expire-time value, shown here, is how much time remained before reaching the timeout interval.

28-7 show ip dvmrp route

This command is used to display DVMRP route information.

show ip dvmrp route [*NETWORK-ADDRESS***]**

Parameters

NETWORK-ADDRESS	(Optional) Specifies the source network address and mask length. If the network address not specified, all DVMRP routes will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display DVMRP route information.

Example

This example shows how to displays route information.

```
Switch# show ip dvmrp route

State: H = Hold-down
Source Network     Upstream Neighbor  Metric  Learned  Interface  State  ExpTime
---------------  -----------------  ------  -------  ---------  -----  ------
10.10.11.0/24     0.0.0.0            1       Local    vlan1       H      -

Total Entries: 1

Switch#
```

Display Parameters

Source Network	The source IP address or source network.
Upstream neighbor	The next hop router to the source network. Use 0.0.0.0 since this route is a local interface entry and does not enable DVMRP. If the interface is a local entry, then the up-stream neighbor displays the interface IP address.
Learned	Indicates this route entry is a local interface. The other condition is dynamically learned.
Interface	The interface to the source network.
State	The route state displays “H” if the DVMRP route is in the “Hold-down” state.
ExpTime	The amount of time remaining until the entry is removed from the DVMRP routing table. A dash note indicates that this entry is not going to be removed (because it is a local interface).

29. D-Link License Management System (DLMS) Commands

29-1 install dlms activation-code

This command is used to install an activation code on the switch.

install dlms activation-code *AC-STR* **[unit** *UNIT-ID***]**

Parameters

AC-STR	Specifies the activation code. The length should be 25 characters.
UNIT-ID	(Optional) Specifies the unit ID of the switch in the switch stack. When the unit ID is not specified, the activation code will be installed on the current switch.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

The license specifies the feature options that are enabled on the switch. License keys are sold in the market. It may be printed on a physical package or be displayed in an e-mail or a portal. The user needs register the license key on the Global Registration Portal to get the activation code. Install the proper activation code rather than license key to activate/unlock some features.

This command is used to install the activation code. After the activation code was installed successfully, reboot the switch to activate the license.

Example

This example shows how to install a legal activation code.

```
Switch# install dlms activation-code xBc7vNWsSpchuQkGZsTfPwcfa

Success.

Please reboot the device to activate the license.

Switch#
```

This example shows an activation code that is illegal.

```
Switch# install dlms activation-code xBc7vNWsSpchuQkGZsTfPwAcb

ERROR: Illegal activation code.

Switch#
```

29-2 show dlms license

This command is used to display the installed DLMS license information on the switch.

show dlms license [unit *UNIT-ID***]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the unit ID of the switch in the switch stack.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command will display the installed DLMS license information on the switch. The device's default license and active license will be displayed for this command. If the optional keyword **unit** is not specified, license information of current switch will be displayed.

Example

This example shows how to display the installed DLMS license information on the switch.

```
Switch# show dlms license

Device Default License : SI
Current Active License : EI

License Model            Activation Code                  Time Remaining
-------------------------------------------------------------------------
DXS-3600-28SC-SE-LIC     xBc7vNWsSpchuQkGZsTfPwAcb        33 weeks
DXS-3600-28SC-SE-LIC     xBc7vNWsSpchuQkGZsTfPwAcc*
DXS-3600-28SC-SE-LIC     xBc7vNWsSpchuQkGZsTfPwAcd*
-------------------------------------------------------------------------
DXS-3600-28SC-SR-LIC     xBc8xTWsQpchxTkGZsTfPwBtt        No Limited
-------------------------------------------------------------------------
  * expired

Switch#
```

Display Parameters

Unit ID	The unit ID of the switch.
Device Default License	The default license mode. The default license will be active when no license is active (For example, when no activation code is installed or all installed activation codes have expired.) SI indicates 'Standard

	License'.
Current Active License	The current license mode. The current active license is the highest level valid license. Current active license specifies the feature options that are enabled on the switch. EI indicates 'Enhance License'.
License Model	The license model name for the installed license.
Activation Code	The activation code for the installed license.
Time Remaining	The time remaining for the installed license. If there is no description and an asterisk (*) is appended to the activation code, the license has expired.

30. D-Link Unidirectional Link Detection (DULD) Commands

30-1 duld enable

This command is used to enable Ethernet OAM unidirectional link detection on the specified port. Use the **no** command to disable the function.

duld enable

no duld enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

D-Link's Unidirectional Link Detection is an extension for 802.3ah Ethernet OAM. It provides a mechanism to detect a unidirectional point-to-point Ethernet link without PHY support. OAM vendor specific messages are used in the detection. The detection process is started after OAM discovery was started but does not complete the negotiation in the configured discovery time.

Example

This example shows how to enable and then disable Ethernet OAM unidirectional link detection on interface 1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# duld enable
Switch(config-if)# no duld enable
Switch(config-if)#
```

30-2 duld action

This command is used to configure the Ethernet OAM unidirectional link detection action on the specified port. To return to the default settings, use the **no** form of this command.

duld action shutdown

no duld action shutdown

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the Ethernet OAM unidirectional link detection action on the specified port.

Example

This example shows how to configure interface 1/0/1's OAM DULD mode to shutdown.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# duld action shutdown
Switch(config-if)#
```

30-3 duld discovery-time

This command is used to configure Ethernet OAM unidirectional link detection discovery time.

duld discovery-time *SECONDS*

no duld discovery-time

Parameters

SECONDS	Specifies the discovery time. The valid range is 5 to 65535.

Default

By default, this value is 5 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the OAM discovery does not successfully negotiate before discovery time expired, OAM unidirectional link detection will start.

Example

This example shows how to configure the DULD discovery time to 7 seconds on interface 1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# duld discovery-time 7
```

```
Switch(config-if)#
```

30-4 show duld

This command is used to display the information of Ethernet OAM unidirectional link detection.

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

Parameters

interface *INTERFACE-ID*	Specifies the interface ID to display. The allowed interfaces only include physical ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command used to display the information of DULD.

Example

This example shows how to display Ethernet OAM unidirectional link detection.

```
Switch# show duld interface eth1/0/1

eth1/0/1
Admin State             : Enabled
Oper Status             : Enabled
Action                   : Shutdown
Link Status             : Bidirectional
Discovery Time(Sec)    : 5

Switch#
```

31. Domain Name System (DNS) Commands

31-1 clear host

This command is used to clear the dynamically learned host entries in the privileged user mode.

clear host {all | [vrf *VRF-NAME*] [*HOST-NAME*]}

Parameters

all	Specifies to clear all host entries.
VRF-NAME	(Optional) Specifies the name of the VRF instance.
HOST-NAME	(Optional) Specifies to delete the specified dynamically learned host entry.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

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#
```

31-2 ip dns server

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

ip dns server

no ip dns server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The system supports the DNS caching name server function. When the caching name server function is enabled and IP domain-lookup, the system forwards the DNS query packet to the configured name server. The answer replied by the name server will be cached and used to answer the subsequent queries.

Example

This example shows how to enable the DNS caching name server function.

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

31-3 ip dns lookup

This command is used to enable DNS searching dynamic cached or static created host entries. Use the **no** form of this command to disable DNS searching dynamic or static host entries.

ip dns lookup [static] [cache]

no ip dns lookup [static] [cache]

Parameters

static	(Optional) Specifies to enable or disable the lookup of static entries before asking the name server.
cache	(Optional) Specifies to enable or disable the lookup of the dynamic cache before asking the name server.

Default

Enable lookup static and cache.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the system tries to lookup a domain name, by default, it will look in the static and dynamic cache first and then send a query to the name server if no matching entries were found. Use this command to disable the lookup option of static or dynamic cache entries before sending requests to the name server. If this command is used without options, then the static and cache options are enabled or disabled at the same time.

Example

This example shows how to enable the lookup of a static host for answering the request.

```
Switch# configure terminal
Switch(config)# ip dns lookup static
```

```
Switch(config)#
```

31-4 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.

Command Default Level

Level: 12.

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)#
```

31-5 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 the command to remove the static host entry.

ip host [vrf *VRF-NAME***]** *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

no ip host [vrf *VRF-NAME***]** *HOST-NAME* **{***IP-ADDRESS* **|** *IPV6-ADDRESS***}**

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.
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.

Command Default Level

Level: 12.

Usage Guideline

The host name specified in this command needs to be qualified. To delete a static host entry, use the **no** command.

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)#
```

31-6 ip name-server

This command is used to configure the IP address of a domain name server. Use the **no** form of this command to delete the configured domain name server.

ip name-server [vrf *VRF-NAME***] {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

no ip name-server [vrf *VRF-NAME***] {***IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.
IP-ADDRESS	Specifies the IPv4 address of the domain name server.
IPV6-ADDRESS	Specifies the IPv6 address of the domain name server.
IP-ADDRESS2…IP-ADDRESS6	Specifies multiple IP addresses, separated by spaces. Up to four servers can be specified.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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. The user can configure up to 4 name servers.

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)#
```

31-7 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 it to the default value.

ip name-server timeout *SECONDS*

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.

Command Default Level

Level: 12.

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)#
```

31-8 show hosts

This command is used to display the DNS configuration.

show hosts [vrf *VRF-NAME***]**

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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: 2
Number of Dynamic Entries: 1

Host Name:    www.yes.com
IP Address:    10.0.0.88
IPv6 Address:  2001:1::1
Age:          1334minutes

Host Name:    www.abc.com
IP Address:    10.0.0.10
Age:           forever

Host Name:    www.greet.com
IPV6 Address:  2001:2::1
Age:           forever

Switch#
```

31-9 show ip name_server

This command is used to display the DNS configuration.

show ip name_server [vrf *VRF-NAME***]**

Parameters

VRF-NAME	(Optional) Specifies the name of the VRF instance.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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

Name servers are: 1.1.1.1
Name servers are: 1000::1
Name servers are: 2.2.2.2
Name servers are: 2000::2

Switch#
```

32. DoS Prevention Commands

32-1 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable 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.

The command **no dos-prevention** with the **all** keyword is used 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.

NOTE: Some functions using the NTP protocol might not function properly when the **Blat** attack DoS prevention type is enabled as they use the same port number.

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)# dos-prevention all
Switch(config)#
```

This example shows how to disable the DoS prevention mechanism for all supported types.

```
Switch# configure terminal
Switch(config)# no dos-prevention all
Switch(config)#
```

32-2 show dos-prevention

This command is used to display the DoS prevention status and related drop counters.

show dos-prevention [*DOS-ATTACK-TYPE***]**

Parameters

DOS-ATTACK-TYPE	(Optional) Specifies the DoS type to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about DoS prevention.

Example

This example shows how to display the configuration information for DoS prevention.

```
Switch# show dos-prevention
```

```
DoS Prevention Information
DoS Type                                 State
---------------------------------------- --------------
Land Attack                              Enabled
Blat Attack                              Enabled
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 configuration information for output land of DoS prevention.

```
Switch# show dos-prevention land

DoS Type    : Land Attack
State        : Enabled

Switch#
```

33. Dynamic ARP Inspection Commands

33-1 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** 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.

Command Default Level

Level: 12.

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 0.0.255.255 mac any
Switch(config-arp-nacl)# permit ip 10.30.0.0 0.0.255.255 mac any
Switch(config-arp-nacl)#
```

33-2 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

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#
```

33-3 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

vlan *VLAN-ID*	(Optional) Specifies the VLAN or range of VLANs.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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#
```

33-4 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** 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 interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and 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.

Command Default Level

Level: 12.

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, the packet will be further matched against the DHCP snooping binding entries if the keyword “static” is not specified. The implicit denied packet is dropped if the keyword “static” is specified.

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)#
```

33-5 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 the command to return 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.

Command Default Level

Level: 12.

Usage Guideline

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 eth3/0/10
Switch(config-if)# ip arp inspection limit rate 30 burst interval 5
Switch(config-if)#
```

33-6 ip arp inspection log-buffer

This command is used to configure the ARP inspection log buffer parameter.

ip arp inspection log-buffer entries *NUMBER*

no ip arp inspection log-buffer entries

Parameters

NUMBER	(Optional) Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the 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, then 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)#
```

33-7 ip arp inspection trust

This command is used to trust an interface for dynamic ARP inspection. Use the **no** form of the command to disable the trust state.

ip arp inspection trust

no ip arp inspection trust

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When an interface is in the trust 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 3/0/3 to be trusted for DAI.

```
Switch# configure terminal
Switch(config)# interface eth3/0/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)#
```

33-8 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 the 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.

Command Default Level

Level: 12.

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 parameters are specified, all options are enabled or disabled. Use the **no** form of the command with the specific option to disable the specific type of check.

Example

This example shows how to enable source MAC validation.

```
Switch# configure terminal
Switch(config)# ip arp inspection validate src-mac
Switch(config)#
```

33-9 ip arp inspection vlan

This command is used to enable specific VLANs for dynamic ARP inspection. Use the **no** form of the command disable dynamic ARP inspection for VLAN.

ip arp inspection vlan *VLAN-ID* **[, | -]**

no ip arp inspection vlan *VLAN-ID* **[, | -]**

Parameters

vlan VLAN-ID	Specifies the VLAN to enable or disable the ARP inspection function.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

By default, ARP inspection is disabled on all VLANs.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

33-10 ip arp inspection vlan logging

This command is used to control the type of packets that are logged. Use the **no** form of the command to revert the setting to default.

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 *VLAN-ID*	Specifies the VLAN to enable or disable the logging control function.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and 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

All denied or dropped packets are logged.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **no** form of this command to reset some of the logging criteria to their defaults. If not specified, all the logging types are reset to log on when the ARP packets are denied.

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)#
```

33-11 permit | deny (arp access-list)

This command is used to define the ARP permit entry. Use the **deny** command to define the ARP deny entry. Use the **no** form of the 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-	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

MASK	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.

Command Default Level

Level: 12.

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)#
```

33-12 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 *INTERFACE-ID*	(Optional) Specifies a port, range of ports or all ports to configure.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
vlan *VLAN-ID*	(Optional) Specifies a VLAN or range of VLANs.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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.

Example

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
----- -------------  ------------------------------ ----------
10      Enabled         -                                        -
VLAN   ACL Logging DHCP Logging
----- ----------- ----------
10      Deny          Deny

Switch#
```

Display Parameters

VLAN	The VLAN ID that enables 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.

Example

This example shows how to display the trust state of interface eth3/0/3.

```
Switch# show ip arp inspection interfaces eth3/0/3

Interface   Trust State   Rate(pps)  Burst Interval
---------   -----------   ---------  --------------
eth3/0/3     untrusted     30           5

Switch#
```

This example shows how to display the trust state of interfaces on the switch.

```
Switch# show ip arp inspection interfaces

Interface   Trust State   Rate(pps)    Burst Interval
---------   -----------   ---------   -------------
eth3/0/1      untrusted    30            1
eth3/0/2      untrusted    30            1
eth3/0/3      untrusted    30            5
eth3/0/5      trusted       None         1
eth3/0/6      untrusted    30            1
eth3/0/7      untrusted    30            1
eth3/0/8      untrusted    30            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.

33-13 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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: 64

Interface   VLAN        Sender IP          Sender MAC        Occurrence
---------- --------  ------------- -----------------  --------------------------
eth1/0/1     100       10.20.1.1      00-20-30-40-50-60     1 (2013-12-28 23:08:66)
eth1/0/2     100       10.5.10.16     55-66-20-30-40-50     2 (2013-12-02 00:11:54)
eth1/0/3     100       10.58.2.30     10-22-33-44-50-60     1 (2013-12-30 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.

34. Enhanced Transmission Selection (ETS) Commands

34-1 ets willing

This command is used to enable the Enhanced Transmission Selection (ETS) willing mode for the Data Center Bridging Exchange Protocol (DCBX) on the specified interface. Use the **no** form of this command to disable the willing mode.

ets willing

no ets willing

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable willing mode for ETS configuration when running DCBX, which indicates that the interface is willing to accept configurations from the remote switch.

DCBX is used by DCB devices to exchange configuration information with directly connected peers. The protocol may also be used for misconfiguration detection and for configuration of the peer.

The willing mode indicates that the local port has been administratively configured to accept configurations from the remote device.

Example

This example shows how to enable the ETS willing option at interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# ets willing
Switch(config-if)#
```

34-2 ets recommend

This command is used to configure the Enhanced Transmission Selection (ETS) recommendation on the specified interface. This setting will be translated to a DCBX ETS recommendation TLV. The TLV is encoded into each LLDP message and may be transmitted by a system in order to indicate a recommendation on how ETS should be configured. Use the **no** form of this command to revert to the default setting.

ets recommend {bandwidth *WEIGHT0 WEIGHT1 WEIGHT2 WEIGHT3 WEIGHT4 WEIGHT5 WEIGHT6 WEIGHT7* **| cos-map** *COS-QUEUE COS-VALUE* **[, | -]}**

no ets recommend [bandwidth | cos-map]

Parameters

bandwidth *WEIGHT0 WEIGHT2 WEIGHT3 WEIGHT4 WEIGHT5 WEIGHT6 WEIGHT7*	Specifies the recommended bandwidth for traffic classes 0 to 7. It is required to specify 8 values for traffic class 0 to 7 respectively. The sum of the bandwidth assigned to a given port is required at all times to be equal to 100. An operation that attempts to change the bandwidth where the sum is not 100 will be rejected. The valid range is from 0 to 100 (in percentage). The value of zero stands for strict priority mode.
cos-map *COS-QUEUE COS-VALUE* **[,	-]**	Specifies the recommended priority assignment table. *COS-QUEUE*: Specifies the queue ID (Traffic Class) for the specified priority. *COS-VALUE*: Specifies the priority to be mapped. The value is from 0 to 7.You can specify multiple priorities queued into the specified traffic class.

Default

The recommended bandwidth is 4, 7, 11, 14, 18, 21, and 25 (in percentage) for traffic classes 0 to 6 respectively. 0 for traffic class 7 means the recommended transmission selection algorithm is “strict priority.

The default priority (CoS) to traffic class mapping is 0 to 1, 1 to 0, 2 to 2, 3 to 3, 4 to 4, 5 to 5, 6 to 6, and 7 to 7.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the recommended bandwidth (in percent) for each traffic class. The value of zero means using “strict priority” for the corresponding traffic class. If the **no ets recommand** command is issued without any keywords, all ETS recommendation settings (bandwidth and priority assignments) will be reverted to the default values.

Example

This example shows how to configure the recommended transmission selection algorithm for traffic classes 0 to 4 is ETS and the allocated bandwidth is 10%, 10%, 20%, 20%, and 40% respectively. For traffic class 5 to 7 the recommended transmission selection algorithm is strict priority.

```
Switch# configure terminal
Switch(config)# interface eth3.1
Switch(config-if)# ets recommend bandwidth 10 10 20 20 40 0 0 0
Switch(config-if)#
```

34-3 show ets interface

This command is used to display the ETS information of a given interface or all interfaces.

show ets interface [*INTERFACE-ID* **[, | -]] [recommend]**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.
recommend	(Optional) Specifies to display the ETS recommendation information of a given interface or all interfaces.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the ETS settings and status on the specified interface(s).

Example

This example shows how to display recommendation information for interface3/0/1.

```
Switch# show ets-recommend interface eth3/0/1 recommend

Interface Id:       eth3/0/1
Recommended TC Setting:
CoS         Mapped CoSs       Scheduler   Bandwidth
Queue ID    (Priorities)      Type        Percentage
----------  ---------------   ---------  ----------
   0        0,1,2,3,4,5,6,7   ETS        30
   1                          ETS        70
   2                          Strict      0
   3                          Strict      0
   4                          Strict      0
   5                          Strict      0
   6                          Strict      0
   7                          Strict      0

Switch#
```

35. Error Recovery Commands

35-1 errdisable recovery

This command is used to enable the error recovery for causes and to configure the recovery interval. Use the **no** 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 | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard} [interval *SECONDS***]**

no errdisable recovery cause {all | psecure-violation | storm-control | bpdu-protect | arp-rate | dhcp-rate | loopback-detect | l2pt-guard} [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.
bpdu-protect	Specifies to enable the auto-recovery option for an error port caused by BPDU protection.
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.
l2pt-guard	Specifies to enable the auto-recovery option for an error port caused by Layer 2 protocol tunneling.
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.

Command Default Level

Level: 12.

Usage Guideline

A port can be put in an error disabled state by causes such as port security violations, storm control, etc…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 psecurity-violation
Switch(config)#
```

35-2 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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
-----------------    -----------   -----------
psecure-violation      enabled     200 seconds
storm-control          disabled    300 seconds
bpdu-protect           disabled    300 seconds
arp-rate               disabled    1000 seconds
dhcp-rate              disabled    1000 seconds
loopback-detect        disabled    1000 seconds
l2pt-guard             disabled    1000 seconds

Interfaces that will be recovered at the next timeout:

Interface    Errdisable Cause    Time left(sec)
```

```
---------    -----------------    --------------
Port1.4      psecure-violation    179

Switch#
```

36. Ethernet OAM Commands

36-1 ethernet oam

This command is used to enable the Ethernet OAM function on the specified port. Use the **no** command to disable the function.

ethernet oam

no ethernet oam

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

After enabling this function on the interface, the interface will start OAM discovery. If the OAM mode of this interface is active, it initiates the discovery. Otherwise, it reacts to the discovery received from the peer.

Example

This example shows how to enable Ethernet OAM on interface eth1/0/1.

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

36-2 ethernet oam mode

This command is used to configure the Ethernet OAM mode on the specified port. To return to the default settings, use the **no** form of this command.

ethernet oam mode {active | passive}

no ethernet oam mode

Parameters

active	Specifies that the port's Ethernet OAM mode is active.
passive	Specifies that the port's Ethernet OAM mode is passive.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The following two actions are allowed by ports in the active mode, but disallowed by ports in the passive mode.

- Initiate OAM discovery.
- Start or stop remote loopback.

Example

This example shows how to configure interface eth1/0/1 Ethernet OAM mode to active.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam mode active
Switch(config-if)#
```

36-3 ethernet oam link-monitor error-symbol

This command is used to enable notifying the Ethernet OAM error symbol event and configure the monitor threshold and window on the specified port. Use the **no** command to disable notifying the event and return the parameters to default value.

ethernet oam link-monitor error-symbol [threshold *NUMBER***] [window** *DECISECONDS***]**

no ethernet oam link-monitor error-symbol [threshold] [window]

Parameters

threshold *NUMBER*	Specifies a number of symbol errors. If symbol errors occur in the specified window and it exceeds the threshold value, then the event is generated. The range is 0 to 4294967295.
window *DECISECONDS*	Specifies the amount of time over which the threshold is defined. If threshold symbol errors occur within the period, an event notification OAM PDU should be generated with an error symbol period event TLV, indicating that the threshold has been crossed in this window. The range is 10 to 600 deciseconds.

Default

The Ethernet OAM error symbol event will be notified by default.

The default Ethernet OAM error symbol monitor threshold is 1.

The default Ethernet OAM error symbol monitor window is 10 deciseconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The link monitoring function counts the number of symbol errors that occur during the specified window period. This event is generated if the symbol error count is equal to or greater than the specified threshold for that period.

Example

This example shows how to enable notifying an Ethernet OAM error symbol events on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol
Switch(config-if)#
```

This example shows how to disable notifying an Ethernet OAM error symbol events on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-symbol
Switch(config-if)#
```

This example shows how to configure the interface eth1/0/1 Ethernet OAM error symbol monitor threshold to 100.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol threshold 100
Switch(config-if)#
```

This example shows how to configure the interface eth1/0/1 Ethernet OAM error symbol monitor window to 100 deciseconds.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-symbol window 100
Switch(config-if)#
```

This example shows how to configure the interface eth1/0/1 Ethernet OAM error symbol monitor threshold to the default value.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-symbol threshold
Switch(config-if)#
```

36-4 ethernet oam link-monitor error-frame

This command is used to enable notifying the Ethernet OAM error frame event and configure the monitor threshold and window on the specified port. Use the **no** command to disable notifying the event or return the parameters to the default value.

ethernet oam link-monitor error-frame [threshold *NUMBER***] [window** *DECISECONDS***]**

no ethenet-oam link-monitor error-frame [threshold] [window]

Parameters

threshold *NUMBER*	Specifies the number of frame errors. If the error frames occur in the specified window and exceeds the threshold value, then an error frame event is triggered. The range is 0 to 4294967295.
window *DECISECONDS*	Specifies the amount of time over which the threshold is defined. If the threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame event TLV, indicating that the threshold has been crossed in this window. The range is 10 to 600 deciseconds.

Default

The Ethernet OAM error frame event shall be notified by default.

The default Ethernet OAM error frame monitor threshold is 1.

The default Ethernet OAM error frame monitor window is 10 deciseconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The link monitoring function counts the number of error frames detected during the specified window period. This event is generated if the error frame count is equal to or greater than the specified threshold for that period.

Example

This example shows how to enable notifying an Ethernet OAM error frame event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame
Switch(config-if)#
```

This example shows how to disable notifying an Ethernet OAM error frame event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame monitor threshold to 100.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame threshold 100
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame monitor window to 100 deciseconds.

```
Switch# configure terminal
```

```
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame window 100
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame monitor window to default value.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame window
Switch(config-if)#
```

36-5 ethernet oam link-monitor error-frame-seconds

This command is used to enable notifying the Ethernet OAM error frame second event and configure the monitor threshold and window on the specified port. Use the **no** command to disable notifying the event or return the parameters to the default value.

ethernet oam link-monitor error-frame-seconds [threshold *NUMBER***] [window** *DECISECONDS***]**

no ethernet oam link-monitor error-frame-seconds [threshold] [window]

Parameters

threshold *NUMBER*	Specifies the number of error frames in seconds. If the number of the error frames occur in the specified window and exceeds the threshold value, then the frame event is triggered. The range is 1 to 900.
window *MILLISECONDS*	Specifies the amount of time over which the threshold is defined. If threshold frame errors occur within the period, an event notification OAM PDU will be generated with an error frame seconds summary event TLV indicating that the threshold has been crossed in this window. The range is 100 to 9000 deciseconds.

Default

The Ethernet OAM error frame seconds event will be notified by default.

The default Ethernet OAM error frame seconds monitor threshold is 1.

The default Ethernet OAM error frame seconds monitor window is 600 deciseconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The link monitoring function counts the number of error frames that occurred during the specified window period. This event is generated if the number of error frames is equal to or greater than the specified threshold for that period. An error frame second is a one second interval wherein at least one frame error was detected.

Example

This example shows how to enable notifying an Ethernet OAM error frame event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

This example shows how to disable notifying an Ethernet OAM error frame event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-seconds
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame seconds monitor threshold to 100.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds threshold 100
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame seconds monitor window to 100 deciseconds.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-seconds window 100
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame seconds monitor threshold to default value.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-seconds threshold
Switch(config-if)#
```

36-6 ethernet oam link-monitor error-frame-period

This command is used to enable notifying the Ethernet OAM error frame period event and configure the monitor threshold and window on the specified port. Use the **no** command to disable notifying the event or return the parameters to the default value.

ethernet oam link-monitor error-frame-period [threshold *NUMBER***] [window** *NUMBER***]**

no ethernet oam link-monitor error-frame-period [threshold] [window]

Parameters

threshold *NUMBER*	Specifies the number of frame errors that must occur for this event to be triggered. The range is 0 to 4294967295.
window *NUMBER*	Specifies the number of frames over which the threshold is defined. If threshold frame errors occur within the period, an event notification

	OAM PDU should be generated with an error frame period event TLV indicating that the threshold has been crossed in this window. The lower bound is the number of minimum frame-size frames that can be received in 100ms on the underlying physical layer. The upper bound is the number of minimum frame-size frames that can be received in one minute on the underlying physical layer.

Default

The Ethernet OAM error frame period event will be notified by default.

The default Ethernet OAM error frame period monitor threshold is 1.

The default window value is the number of minimum frame-size frames that can be received in one second on the underlying physical layer.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The link monitoring function counts the number of error frames detected during the specified period. The period is specified by a number of received frames. This event is generated if the error frame count is greater than or equal to the specified threshold for that period

Example

This example shows how to enable notifying an Ethernet OAM error frame period event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

This example shows how to disable notifying and Ethernet OAM error frame period event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame-period
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame period monitor threshold to 100.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period threshold 100
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame period monitor window to 1488100 frames.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam link-monitor error-frame-period window 1488100
Switch(config-if)#
```

This example shows how to configure interface eth1/0/1 Ethernet OAM error frame period monitor threshold to default value.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no ethernet oam link-monitor error-frame- period threshold
Switch(config-if)#
```

36-7 ethernet oam remote-failure dying-gasp

This command is used to enable notifying the dying gasp event on the specified port. Use the **no** command to disable the function.

ethernet oam remote-failure dying-gasp

no ethernet oam remote-failure dying-gasp

Parameters

None.

Default

The Ethernet OAM dying gasp event will be notified by default.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command used to configure the capability of the dying gasp event. If the capability for the dying gasp event is disabled, the port will never send out OAM PDUs with the dying gasp event bit set when an unrecoverable local failure condition has occurred.

Example

This example shows how to enable the notifying dying gasp event on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam remote-failure dying-gasp
Switch(config-if)#
```

36-8 ethernet oam remote-failure critical-event

This command is used to enable notifying the critical event on the specified port. Use the **no** command to disable the function.

ethernet oam remote-failure critical-event

no ethernet oam remote-failure critical-event

Parameters

None.

Default

The Ethernet OAM critical event will be notified by default.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command used to configure the capability of the critical event. If the capability for a critical event is disabled, the port will never send out OAM PDUs with critical event bit set when an unspecified critical event has occurred.

Example

This example shows how to enable notifying critical events on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam remote-failure critical-event
Switch(config-if)#
```

36-9 ethernet oam remote-loopback

This command is used to set the action of the remote loopback on the specified port.

ethernet oam remote-loopback {start | stop} interface *INTERFACE-ID* **[, | -]**

Parameters

start	Specifies to request the peer to change to the remote loopback mode.
stop	Specifies to request the peer to change to the normal operation mode.
interface *INTERFACE-ID*	Specifies the ID of an interface to do the remote loopback action. The allowed interfaces only include physical ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to request the remote peer to enter or exit the Ethernet OAM remote loopback mode. Use the **ethernet oam remote-loopback start** command to request the remote peer to enter the Ethernet OAM remote loopback mode. Use the **ethernet oam remote-loopback stop** command to request the remote peer to exit the Ethernet OAM remote loopback mode.

If the remote peer is configured to ignore the remote loopback request, then the remote peer will not enter or exit the remote loopback mode upon receiving the request. To start the remote peer to enter the remote loopback mode, administrators must ensure that the local client is in the active mode and the OAM connection is established. If the local client is already in the remote loopback mode, then this command cannot be applied.

Example

This example shows how to start the Ethernet OAM remote loopback on interface eth1/0/1.

```
Switch# ethernet oam remote-loopback start interface eth1/0/1
Switch#
```

36-10 ethernet oam received-remote-loopback

This command is used to configure the behavior of the received remote loopback requirement from the peer on the specified port. To return to the default settings, use the **no** form of this command.

ethernet oam received-remote-loopback {process | ignore}

Parameters

process	Specifies to react to remote loopback requirements from a peer.
ignore	Specifies not to react to remote loopback requirements from a peer.

Default

The Ethernet OAM ignores remote loopback requirement by default.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In the remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering the remote loopback mode.

Example

This example shows how to enable processing the Ethernet OAM remote loopback command on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# ethernet oam received-remote-loopback process
Switch(config-if)#
```

36-11 show ethernet oam configuration

This command is used to display the configuration of the Ethernet OAM function.

show ethernet oam configuration [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID to display. The allowed interfaces will only include the physical port.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is used to display port Ethernet OAM configurations.

Example

This example shows how to displays the Ethernet OAM configuration of interface eth1/0/1.

```
Switch# show ethernet oam configuration interface eth1/0/1

eth1/0/1
 Ethernet oam state     : Disabled
 Mode                   : Active
 Dying gasp             : Enabled
 Critical event         : Enabled
 Remote loopback OAMPDU : Processed
Error symbol period event
 Notify state           : Enabled
 Threshold              : 1 error symbol
 Window                 : 10 deciseconds
Error frame event
 Notify state           : Enabled
 Threshold              : 1 error frame
 Window                 : 10 deciseconds
Error frame period event
 Notify state           : Enabled
 Threshold              : 1 error frame
 Window                 : 100 (in 10000 frames)
```

```
Error frame seconds event
 Notify state           : Enabled
 Threshold              : 1 error frame
 Window                 : 600 deciseconds

Switch#
```

36-12 show ethernet oam status

This command is used to display the status of the Ethernet OAM function.

show ethernet oam status [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID to display. The allowed interfaces only include physical ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

The command used to display primary controls and status information for Ethernet OAM on specified ports.

Example

This example shows how to display the Ethernet OAM status of interface eth1/0/1.

```
Switch# show ethernet oam status interface eth1/0/1

eth1/0/1
 Local client
  Admin State                 : Enabled
  Mode                        : Active
  Max OAMPDU size             : 1518 bytes
  Remote loopback             : Support
  Unidirectional              : Not support
  Link monitoring             : Support
  Variable request            : Not support
  PDU revision                : 1
  Operation status            : Operational
```

```
  Loopback status               : No loopback
 Remote client
  Mode                          : Passive
  MAC address                   : 0001.0203.0405
  Vendor (OUI)                  : 0180c2
  Max OAMPDU size               : 1518 bytes
  Unidirectional                : Support
  Link monitoring               : Support
  Variable request              : Support
  PDU revision                  : 1

Switch#
```

Display Parameters

Operation status	**Disable:** OAM is disabled on this port **LinkFault:** The link has detected a fault and is transmitting OAMPDUs with a link fault indication. **PassiveWait:** The port is passive and is waiting to see if the peer device is OAM capable. **ActiveSendLocal:** The port is active and is sending local information **SendLocalAndRemote:** The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer. **SendLocalAndRemoteOk:** The local device agrees the OAM peer entity. **PeeringLocallyRejected:** The local OAM entity rejects the remote peer OAM entity. **PeeringRemotelyRejected:** The remote OAM entity rejects the local device. **Operational:** The local OAM entity learns that both it and the remote OAM entity have accepted the peering. **NonOperHalfDuplex:** Since Ethernet OAM functions are not designed to work completely over half-duplex port. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.
Max OAMPDU size	The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers.
PDU revision	The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The configuration revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.
Unidirectional	It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
Remote loopback	It indicates that the OAM entity can initiate and respond to loopback commands.
Link Monitoring	It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
Variable request	It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB

36-13 show ethernet oam statistics

This command is used to display the statistics of the Ethernet OAM function.

show ethernet oam statistics [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID to display. The allowed interfaces only include physical ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is used to display port Ethernet OAM statistics.

Example

This example shows how to display the Ethernet OAM statistics of interface eth1/0/1.

```
Switch# show ethernet oam statistics interface eth1/0/1

eth1/0/1
 Information OAMPDU TX                                : 0
 Information OAMPDU RX                                : 0
 Unique event notification OAMPDU TX                  : 0
 Unique event notification OAMPDU RX                  : 0
 Duplicate event notification OAMPDU TX               : 0
 Duplicate event notification OAMPDU RX               : 0
 Loopback control OAMPDU TX                           : 0
 Loopback control OAMPDU RX                           : 0
 Variable request OAMPDU TX                           : 0
 Variable request OAMPDU RX                           : 0
 Variable response OAMPDU TX                          : 0
 Variable response OAMPDU RX                          : 0
 Organization specific OAMPDU TX                      : 0
 Organization specific OAMPDU RX                      : 0
 Unsupported OAMPDU TX                                : 0
 Unsupported OAMPDU RX                                : 0
 Frame lost due to OAM                                : 0
```

```
Switch#
```

36-14 clear ethernet oam statistics

This command is used to clear the statistics of the Ethernet OAM function.

clear ethernet oam statistics {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear statistics of all interfaces.
interface *INTERFACE-ID*	Specifies the interface ID to clear. The allowed interfaces only include physical ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to clear port Ethernet OAM statistics.

Example

This example shows how to clear the Ethernet OAM statistics of interface eth1/0/1.

```
Switch# clear ethernet oam statistics interface eth1/0/1
Switch#
```

36-15 show ethernet oam event-log

This command is used to display the event log of the Ethernet OAM function.

show ethernet oam event-log [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID to display. The allowed interfaces only include physical ports.

,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display a port's Ethernet OAM event log.

Example

This example shows how to display the Ethernet OAM event log of interface eth1/0/1.

```
Switch# show ethernet oam event-log interface eth1/0/1

eth1/0/1
    Local Faults:
    -------------
      0 Link Fault records
      0 Dying Gasp records
      0 Critical Event records

    Remote Faults:
    --------------
      0 Link Fault records
      2 Dying Gasp records
        Event  index              : 2
        Time stamp                : 2013.04.18 10:30
        Event  index              : 1
        Time stamp                : 2013.04.18 10:20
    0 Critical Event records

    Local event logs:
    -----------------
      0 Errored Symbol records
      0 Errored Frame records
      0 Errored Frame Period records
      0 Errored Frame Second records

    Remote event logs:
    ------------------
      0 Errored Symbol records
      1 Errored Frame records
   Event  index                       :  3
   Time stamp                         :  2013.04.18 10:31
   Error frame                        :  5
```

```
   Window                              :  10 (decisecond)
   Threshold                           :  3
   Accumulated errors                  : 10
      0 Errored Frame Period records
      0 Errored Frame Second records

Switch#
```

Display Parameters

Event index	When event was generated each event had the index.
Time stamp	The time reference when the event was generated.
Error frame	The number of detected error frames in the period.
Window	The duration of the period in terms of 100ms intervals.
Threshold	The number of detected error frames in the period is required to be equal to or greater than in order for the event to be generated.
Accumulated errors	The sum of error records that have been detected in this event since the OAM sub-layer was reset.

36-16 clear ethernet oam event-log

This command is used to clear the event log of the Ethernet OAM function.

clear ethernet oam event-log {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear the event log of all interfaces.
interface *INTERFACE-ID*	Specifies the interface ID to clear. The allowed interfaces only include physical ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear a port's Ethernet OAM event log.

Example

This example shows how to clear the Ethernet OAM event log of interface eth1/0/1.

```
Switch# clear ethernet oam event-log interface eth1/0/1
Switch#
```

37. Ethernet Ring Protection Switching (ERPS) Commands

37-1 description

This command is used to specify a string that serves as a description for a G.8032 Ethernet ring instance.

description *DESCRIPTION*

Parameters

DESCRIPTION	Specifies the description for a G.8032 Ethernet ring instance with a maximum of 64 characters.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to set the description string for an ERP instance.

Example

This example shows how to create an ERP instance 1 in the physical ring named “major-ring” and add a description for the instance.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erp)# instance 1
Switch(config-erp-instance)# description  major-ring instance 1
Switch(config-erp-instance)#
```

37-2 ethernet ring g8032

This command is used to create a G.8032 physical ring and enter the ERP configuration mode. Use the **no** form of this command to delete the G.8032 physical ring.

ethernet ring g8032 *RING-NAME*

no ethernet ring g8032 *RING-NAME*

Parameters

RING-NAME	Specifies the name of the G.8032 ring with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the Ethernet ring G.8032 command to create or modify a G.8032 ring and enter the ERP configuration mode. The ring created by the command represents a physical ring.

Example

This example shows how to create a G.8032 ring named major-ring.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erp)#
```

37-3 ethernet ring g8032 profile

This command is used to create a G.8032 profile and enter the G.8032 profile configuration mode. Use the **no** form of this command to delete a G.8032 profile.

ethernet ring g8032 profile *PROFILE-NAME*

no ethernet ring g8032 profile *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the G.8032 profile with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create or modify a G.8032 profile and enter the G.8032 profile configuration mode.

Example

This example shows how to create a G.8032 profile named “campus”.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-g8032–ring-profile)# timer guard 700 hold-off 1 wtr 1
Switch(config-g8032–ring-profile)#
```

37-4 tcn-propagation

This command is used to enable the propagation of topology change notifications from the sub-ERP instance to the major instance. Use the **no** form of this command to disable the propagation of topology change notifications.

tcn-propagation

no tcn-propagation

Parameters

None.

Default

By default, this option is disabled.

Command Mode

G.8032 Profile Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the propagation of topology change notifications from the sub-ring instance to other ring instances.

Example

This example shows how to enable the TCN propagation state for the G.8032 profile “campus”.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-g8032–ring-profile)# tcn-propagation
Switch(config-g8032–ring-profile)#
```

37-5 r-aps channel-vlan

This command is used to specify the APS channel VLAN for an ERP instance. Use the **no** form of the command to remove the configuration.

r-aps channel-vlan *VLAN-ID*

no r-aps channel-vlan

Parameters

VLAN-ID	Specifies the VLAN ID of the APS channel VLAN for the ERP instance. The valid range is from 1 to 4094.

Default

None.

Command Mode

ERP Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to assign the APS channel VLAN for an ERP instance. The APS channel VLAN needs to be assigned before an ERP instance can be set to operation state.

The specified APS channel VLAN needs to exist before the instance can be set to operation state.

If the APS channel VLAN is removed when the ERP instance is in operation, the ERP instance will enter operational disabled state.

Each ERP instances should have a distinct APS channel VLAN.

The APS channel VLAN of a sub-ring instance is also the virtual channel of the sub-ring.

Example

This example shows how to configure the APS channel VLAN of the ERP instance 1 as VLAN 2.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erp)# sub-ring ring2
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# port0 interface eth3/0/1
Switch(config-erp)# port1 none
Switch(config-erp)# instance 1
Switch(config-erp-instance)# r-aps channel-vlan 2
Switch(config-erp-instance)#
```

37-6 inclusion-list vlan-ids

This command is used to define a set of Virtual LAN (VLAN) IDs that are protected by the Ethernet ring protection mechanism. To delete the set of VLAN IDs, use the **no** form of this command.

inclusion-list vlan-ids *VLAN-ID* **[, | -]**

no inclusion-list vlan-ids *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the VLAN ID of the service protected VLANs of the ERP instance. The valid range from is1 to 4094.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

ERP Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the VLANs to be protected by the ERP instance.

Example

This example shows how to configure the service protected VLAN as 100 to 200 for ERP instance 1.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# instance 1
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps)# sub-ring ring2
Switch(config-erps)# exit
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# port0 interface eth3/0/1
Switch(config-erp)# port1 none
Switch(config-erp)# instance 1
Switch(config-erp-instance)# r-aps channel-vlan 20
Switch(config-erp-instance)# inclusion-list vlan-ids 100-200
Switch(config-erp-instance)#
```

37-7 instance

This command is used to create an ERP instance and enter the ERP Instance Configuration Mode. Use the **no** form of the command to remove an ERP instance.

instance *INSTANCE-ID*

no instance *INSTANCE-ID*

Parameters

INSTANCE-ID	Specifies the identifier of an ERP instance. This value must be between 1 and 32.

Default

None.

Command Mode

ERP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create an ERP instance under a physical ring. Deploy multiple instances in the same physical ring topology provide the load balancing capability. The ID of ERP instances in physical rings of the system are global significant.

Example

This example shows how to create an ERP instance 1 in the physical ring named “major-ring”.

```
Switch# configure terminal
Switch(config)# ethernet_ring  g8032 major-ring
Switch(config-erp-instance)# instance 1
Switch(config-erp-instance)#
```

37-8 level

This command is used to configure the ring MEL value of an ERP instance. Use the **no** form of this command to return to the default setting.

level *MEL-VALUE*

no level

Parameters

MEL-VALUE	Specifies the ring MEL value of the ERP instance. The valid range is from 0 to 7.

Default

By default, this value is 1.

Command Mode

ERP Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The configured ring MEL value of all ring nodes participating in the same ERP instance should be the identical.

Example

This example shows how to configure the ring MEL value of ERP instance 1 as 6.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config)# sub-ring ring2
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# port0 interface eth3/0/1
Switch(config-erp)# port1 none
Switch(config-erp)# instance 1
Switch(config-erp-instance)# level 6
Switch(config-erp-instance)#
```

37-9 sub-ring

This command is used to specify the sub-ring of a physical ring. Use the **no** form of the command to remove the sub-ring of a physical ring.

sub-ring *SUB-RING-NAME*

no sub-ring *SUB-RING-NAME*

Parameters

SUB-RING-NAME	Specifies the sub-ring's name.

Default

None.

Command Mode

ERP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Configure a sub-ring connected to another ring. This command is applied on the interconnection node.

Example

This example shows how to configure the physical ring named "ring2" as a sub-ring of "ring1".

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# exit
Switch(config)# ethernet ring g8032 ring1
Switch(config-erp)# sub-ring ring2
Switch(config-erp)#
```

37-10 profile

This command is used to associate an ERP instance with a G.8032 profile. Use the **no** form of the command to remove the association.

profile *PROFILE-NAME*

no profile *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the G.8032 profile to be associated with the ERP instance.

Default

None.

Command Mode

ERP Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Multiple ERP instances can be associated with the same profile. Generally, the instances associated with the same G.8032 profile protect the same set of VLANs or the set of VLANs protected by one instance is a subset of LANs protected by another instance. To change the profile association, deactivate the ERP instance first.

Example

This example shows how to configure the guard timer to 700 milliseconds, hold-off timer to 1, WTR timer to 1 minutes for profile “campus”, and then associate instance 1 and 2 with the profile.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-g8032–ring-profile)# timer guard 700 hold-off 1 wtr 1
Switch(config-g8032–ring-profile)#
Switch(config)# ethernet ring g8032 ring1
Switch(config-erp)# port0 interface eth3/0/1
Switch(config-erp)# port1 interface eth3/0/2
Switch(config-erp)# instance 1
Switch(config-erp-instance)# profile campus
Switch(config-erp-instance)#
Switch(config)# ethernet ring g8032 ring2
Switch(config)# ethernet ring g8032 ring1
Switch(config-erp)# sub-ring ring2
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# port0 interface eth3/0/3
Switch(config-erp)# port1 none
Switch(config-erp)# instance 2
Switch(config-erp-instance)# profile campus
Switch(config-erp-instance)#
```

37-11 port0

This command is used to specify the first ring port of a physical ring. To remove the first ring port setting, use the **no** form of this command.

port0 interface *INTERFACE-ID*

no port0

Parameters

INTERFACE-ID	Specifies the interface ID of the configured ring port. It can be physical port or port-channel interface.

Default

None.

Command Mode

ERP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the first ring port of a physical ring.

Example

This example shows how to configure the interface eth3/0/1 as the first ring port of the G.8032 ring “major-ring”.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erp)# port0 interface eth3/0/1
Switch(config-erp)#
```

37-12 port1

This command is used to specify the second ring port of a physical ring. To remove the second ring port setting, use the **no** form of this command.

port1 {interface *INTERFACE-ID* **| none}**

no port1

Parameters

INTERFACE-ID	Specifies the second ring port. It can be a physical port or port-channel interface.
none	Specifies none to indicate that the interconnect node is a local node endpoint of an open ring.

Default

None.

Command Mode

ERP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the second ring port of a physical ring. Use the **port1 none** command to indicate that the interconnect node is a local node endpoint of an open ring.

Example

This example shows how to configure the interconnect node as a local end node of the G.8032 ring “ring2”.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 ring2
Switch(config)# ethernet ring g8032 ring1
Switch(config-erps)# sub-ring ring2
Switch(config-erps)# exit
```

```
Switch(config)# ethernet ring g8032 ring2
Switch(config-erp)# port1 none
Switch(config-erp)#
```

37-13 revertive

This command is used to restore to the working transport entity, in the case of the clearing of a defect. Use the **no** form of the command to continue to use the RPL, if it is not failed, after the switch link defect condition has cleared.

revertive

no revertive

Parameters

None.

Default

By default, this option is enabled.

Command Mode

G.8032 Profile Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In the case of clearing a defect, the traffic channel reverts after the expiry of the WTR timer, which is used to avoid toggling protection states in the case of intermittent defects. In non-revertive operation, the traffic channel continues to use the RPL, if it is not failed, after a switch link defect condition has cleared.

Since in Ethernet ring protection the working transport entity resources may be more optimized, in some cases it is desirable to revert to this working transport entity once all ring links are available.

This is performed at the expense of an additional traffic interruption. In some cases, there may be no advantage to revert to the working transport entities immediately. In this case, a second traffic interruption is avoided by not reverting protection switching.

Example

This example shows how to configure rings in the ring profile “campus” to operate in the non-revertive mode.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-g8032–ring-profile)# no revertive
Switch(config-g8032–ring-profile)#
```

37-14 rpl

This command is used to configure the node as the RPL owner, neighbor and assign the RPL port. Use the **no** form of this command to remove the RPL related setting.

rpl {port0 | port1} {owner}

no rpl

Parameters

port0	Specifies port 0 as the RPL port.
port1	Specifies port 1 as the RPL port.
owner	Specifies the ring node as the RPL owner node for the configured instance.

Default

None.

Command Mode

ERP Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the ring node as the RPL owner node or neighbor node or next neighbor nod of the configured instance and the ring port that acts as the RPL port.

Example

This example shows how to enable the RPL owner and configure port 0 as the RPL port of ERP instance 1.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erp)# port0 interface eth3/0/1
Switch(config-erp)# port1 interface eth3/0/2
Switch(config-erp)# instance 1
Switch(config-erp-instance)# rpl port0 owner
Switch(config-erp-instance)#
```

37-15 show ethernet ring g8032

This command is used to display information of the ERP instance.

show ethernet ring g8032 {status | brief}

Parameters

status	Specifies to display the status of ERP instances.
brief	Specifies to display brief information of ERP instances.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use the **show ethernet ring g8032 brief** command to display brief information of ERP instances.

Use the **show ethernet ring g8032 status** command to display status information of ERP instances.

Example

This example shows how to display detailed information of ERP instances.

```
Switch# show ethernet ring g8032 status

Ethernet ring “Major-Ring”,instance 1,
-----------------------------------
Description: campus instance 1
MEL: 1
Connect sub-ring: ”Sub-Ring”
R-APS Channel: 2, Protected VLAN: 10-20
Profile: Campus
Guard timer: 500 milliseconds
Hold-Off timer: 0 milliseconds
WTR timer: 5 minutes
Non-revertive
Instance State: Idle
Admin RPL ：None
Operational RPL ：None
Admin  Port0: eth3/0/1
Operational Port0: eth3/0/1,
Port0 State: Blocking
Admin  Port1: eth3/0/2
Operational Port1: eth3/0/2
Port1 State:Forwarding
Admin RPL Port : Port0
Operational RPL Port : Port0

Ethernet ring “Sub-Ring”, instance 2
-----------------------------------
Description: campus instance 2
MEL: 2
Connect morjor ring: ”Major-Ring”
R-APS Channel: 2, Protected VLAN: 10-20
profile: Campus
Guard timer: 500 milliseconds
Hold-Off timer: 0 milliseconds
WTR timer: 5 minutes
Non-revertive
No TC propagation
Instance State: Deactivated
Admin  RPL ：-
Operational RPL ：-
Admin  Port0: eth3/0/3
Operational Port0: eth3/0/3
Port0 State:-
```

```
Admin  Port1: none
Operational Port1:none
Port1 State:-
Admin RPL Port : Port0
Operational RPL Port : Port0

Total Entries: 2

Switch#
```

Display Parameters

MEL	The ring MEL value of the ERP instance.
R-APS Channel	The APS channel of the ERP instance.
Protected VLANs	The service protected VLANs of the ERP instance.
Profile	The profile associated with the ERP instance.
Guard timer	The time value for the guard timer of the profile.
Hold-Off timer	The time value for the hold-off timer of the profile.
WTR timer	The time value for the WTR timer of the profile.
TC propagation/No TC Propagation	TC is propagated or not propagated in the profile.
Revertive/Non-Revertive	The ring instance is operated revertively or non-revertively in the profile.
Instance State	The current ring node status of ERP instance. Deactivated / Init / Idle / Protection.
Admin/Operational RPL	The current configuration or running configuration ring node role of ERPS instance. (Owner/None)
Admin/Operational Port0/port1	The current configuration or running configuration ring port role. (Interface ID/none)
Admin/Operational RPL Port	The current configuration or running RPL. (port0/port1/none)
Ring port0/port1 state	The state for ring ports of the ERP instance. (- / Forwarding / Blocked l)

Example

This example shows how to display instance information of all created ERPS domains.

```
Switch# show ethernet ring g8032 brief

Profile           Inst ID    Status           Port-State
------------- --------   ---------        ------------------
Campus              1          Idle              P0: eth3/0/1,Blocked (RPL)
 P1: eth3/0/3,Forwarding
Campus              2          Protection      P0: eth3/0/3,Blocked
 P1:  -
Corportate         3          Deactivated     P0: -
                                                          P1: -
Total Entries: 3
```

```
Switch#
```

Display Parameters

Profile	The profile associated with the ring instances.
Inst ID	The instance identifier of the ERP instance.
RingType	Indicates either the major ring or sub-ring.
Node Type	The RPL owner or neighbor.
Status	The current status of the ERP instance. It can be one of the following values: **Deactivated:** The ERP instance is deactivated. **Init:** The instance is initializing. **Idle:** The instance is in the normal state. The RPL port is blocked. **Protection:** The instance detects failure at some ring port. The RPL port is restored to protect the port.
Port-State	The current ring ports state. (- / Forwarding / Blocked)

37-16 activate

This command is used to activate an ERP instance. Use the **no** activate command to deactivate an ERP instance.

activate

no activate

Parameters

None.

Default

By default, this option is disabled.

Command Mode

ERP Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to activate an ERP instance. The ring ports, APS channel, and profile must be configured first before an ERP instance can be activated. An ERP instance that is activated will be put in non-operational state if the following conditions occur.

- The configured APS channel VLAN does not exist.
- The configured ring ports are not the tagged member port of the APS channel VLAN.

In addition to these configurations, the configuration of service protected VLANs and RPL related settings are fundamental for operation of an ERP instance.

Example

This example shows how to activate the major ring instance 1.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 major-ring
Switch(config-erp)# instance 1
Switch(config-erp-instance)# profile campus
Switch(config-erp-instance)# activate
Switch(config-erp-instance)#
```

37-17 timer

This command is used to configure timers for an ERP domain. Use the **no** form of this command to reset the timer to the default setting.

timer {guard *MILLI-SECONDS* **|hold-off** *SECONDS* **| wtr** *MINUTES***}**

no timer {guard | hold-off | wtr}

Parameters

guard *MILLI-SECONDS*	(Optional) Specifies the guard timer in milliseconds. The valid range is from 10 to 2000. The value should be multiples of 10.
hold-off *SECONDS*	(Optional) Specifies the hold-off timer in seconds. The valid range is from 0 to 10.
wtr *MINUTES*	(Optional) Specifies the WTR timer in minutes. The valid range is from 1 to 12.

Default

The default guard timer is 500 milliseconds.

The default hold-off timer is 0.

The default WTR timer is 5 minutes.

Command Mode

G.8032 Profile Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the timers to be used by ERP instances associated with the profile. Use the **no** command to reset the timer to the default setting. If no option is specified for the **no** command, all timers will be reset.

Example

This example shows how to configure the guard timer to 700 milliseconds, hold-off timer to 1, and WTR timer to 1 minute for profile “campus”.

```
Switch# configure terminal
Switch(config)# ethernet ring g8032 profile campus
Switch(config-g8032–ring-profile)# timer guard 700
Switch(config-g8032–ring-profile)# timer hold-off 1
Switch(config-g8032–ring-profile)# timer wtr 1
Switch(config-g8032–ring-profile)#
```

38. Expansion Module Commands

38-1 port-mode

This command is used to configure the expansion module's port mode.

port-mode unit *UNIT-ID* **{1st_port | 2nd_port | 3rd_port | 4th_port} {4*10giga | 40giga}**

Parameters

UNIT-ID	Specifies the switch's unit ID.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for the DXS-3600-EM-4QXS expansion module. Use this command to configure the port to one 40GBASE-CR4 port or four 10GBASE-R ports.

Example

This example shows how to configure the 2nd port on unit 2 to four 10GBASE-R ports.

```
Switch# configure terminal
Switch(config)# port-mode unit 2 2nd_port 4*10giga
Switch(config)#
```

38-2 show module-info

This command is used to display the expansion module's information.

show module-info [unit *UNIT-ID***]**

Parameters

UNIT-ID	Specifies the switch unit ID.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the expansion module's information.

Example

This example shows how to display the expansion module's information:

```
Switch# show module-info unit 1

Unit 1
Boot-UP Expansion Module SN: 212131652424190
Boot-UP Expansion Module (1):   DXS-3600-EM-8T
Equipped Expansion Module SN: 212131652424190
Equipped Expansion Module (1):  DXS-3600-EM-8T
4QXS Port Mode Configuration:
     1st port mode:40G
     2nd port mode:40G
     3rd port mode:40G
     4th port mode:40G

Switch#
```

This example shows how to display the expansion module's information:

```
Switch# show module-info

Unit 1
Boot-UP Expansion Module SN: 212131652424190
Boot-UP Expansion Module (1):   DXS-3600-EM-4QXS
     1st port mode:4*10G
     2nd port mode:4*10G
     3rd port mode:40G
     4th port mode:40G
Equipped Expansion Module SN: 2345003344443
Equipped Expansion Module (1):  DXS-3600-EM-4QXS
     1st port mode:40G
     2nd port mode:40G
     3rd port mode:40G
     4th port mode:40G
4QXS Port Mode Configuration:
     1st port mode:4*10G
     2nd port mode:40G
     3rd port mode:40G
     4th port mode:40G

Unit 2
Boot-UP Expansion Module SN: 66211165242619925
Boot-UP Expansion Module (1):   DXS-3600-EM-4QXS
     1st port mode:40G
     2nd port mode:40G
     3rd port mode:40G
     4th port mode:40G
Equipped Expansion Module SN: 453344541343443
Equipped Expansion Module (1):  DXS-3600-EM-4QXS
     1st port mode:4*10G
```

```
     2nd port mode:4*10G
     3rd port mode:40G
     4th port mode:40G
4QXS Port Mode Configuration:
     1st port mode:40G
     2nd port mode:4*10G
     3rd port mode:40G
     4th port mode:40G

Switch#
```

39. File System Commands

39-1 cd

This command is used to change the current directory.

cd [*DIRECTORY-URL***]**

Parameters

DIRECTORY-URL	Specifies the URL of the directory. If not specified, the current directory will be shown.

Default

The default current directory is the root directory on the file system of the local FLASH.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If the URL is not specified, then the current directory is not changed.

Example

This example shows how to change the current directory to the directory “log” on file system “c:/”.

```
Switch# dir

Directory of /c:
1 d             0 Dec 29 2013 17:49:36  images
2 d             0 Jan 02 2013 18:42:53  configurations
3 d             0 Jan 02 2013 18:42:53  log
4 -           639 Jan 03 2013 12:09:32  new_config.cfg

20578304 bytes total (3104544 bytes free)

Switch#cd c:/log
Switch#dir

Directory of /c:/log
No files in directory
20578304 bytes total (3104544 bytes free)

Switch#
```

This example shows how to display the current directory.

```
Switch# cd

Current directory is /c:/log
```

```
Switch#
```

39-2 delete

This command is used to to delete a file.

delete *FILE-URL*

Parameters

FILE-URL	Specifies the name of the file to be deleted.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

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 “test.txt” from file system on the local flash.

```
Switch# delete c:/test.txt

Delete test.txt? (y/n) [n] y
File is deleted

Switch#
```

39-3 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.

Command Default Level

Level: 1.

Usage Guideline

If URL is not 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 /
1 d--             0 Jun 31 2013 17:49:36  c:
2 d--             0 Jun 31 2013 18:42:53  d:
0 bytes total (0 bytes free)

Switch#
```

39-4 format

This command is used to format the external storage device.

format *FILE-SYSTEM* **[fat32 | fat16]**

Parameters

FILE-SYSTEM	Specifies the file system.
fat32	(Optional) Specifies to format to the FAT32 file system. This is the default format.
fat16	(Optional) Specifies to format to the FAT16 file system.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Only the external storage can be formatted. The selected storage will be formatted to FAT32 file system by default.

Example

This example shows how to format an external Compact Flash card.

```
Switch# format /d:

All sectors will be erased, proceed? (y/n) [n] y
Enter volume id (up to 11 characters):Profiles
Format completed.

Switch#
```

39-5 mkdir

This command is used to create a directory under the current directory.

mkdir *DIRECTORY-NAME*

Parameters

DIRECTORY-NAME	Specifies the name of the directory.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to make a directory in the current directory.

Example

This example shows how to create a directory named “newdir” under the current directory.

```
Switch# mkdir newdir
Switch#
```

39-6 more

This command is used to display the contents of a file.

more *FILE-URL*

Parameters

FILE-URL	Specifies the URL for the file to be displayed.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the contents of a file in the file system. The command is usually used to display text files. If the content of a file contains non-standard printable characters, the display will feature unreadable characters or even blank spaces.

Example

This example shows how to display the contents of file “usr_def.conf”.

```
Switch# more  /c:/configuration/usr_def.conf

!DXS-3600
!Firmware Version:2.00.012
!Slot      Model
!------ ------------------
! 1        DXS-3600-32S
! 2        -
! 3        DXS-3600-32S
! 4        DXS-3600-32S
!
ip igmp snooping vlan 1
!.
end

Switch#
```

39-7 rename

This command is used to rename a file.

rename *FILE-URL1 FILE-URL2*

Parameters

FILE-URL1	Specifies the URL for the file to be renamed.
FILE-URL2	Specifies the URL after file renaming.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

A file can be renamed to a file located either within the same directory or to another directory.

Example

This example shows how to rename file called “doc.1” to “test.txt”.

```
Switch# rename /c:/doc.1 /c:/test.txt

Rename file doc.1 to text.txt? (y/n) [n] y

Switch#
```

39-8 rmdir

This command is used to remove a directory in the file system.

rmdir *DIRECTORY-NAME*

Parameters

DIRECTORY-NAME	Specifies the name of the directory.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to remove a directory in the working directory.

Example

This example shows how to remove a directory called “newdir” under the current directory.

```
Switch# rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

Switch#
```

39-9 show storage media-info

This command is used to display the storage media’s information.

show storage media-info [unit *UNIT-ID***]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the unit ID in the stacking system. If not specified, all units are displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 on all units.

```
Switch# show storage_media_info

Unit  Drive  Media-Type  Size     FS-Type   Label
----  -----  ----------  -------  --------  -------------
 1    c:     FLASH       31M      FFS
 2    c:     FLASH       31M      FFS
 2    d:     SD Card     256M     FAT32     test
 3    c:     FLASH       31M      FFS

Switch#
```

40. Filter Database (FDB) Commands

40-1 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*	Specifies 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Using this command only clears 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#
```

40-2 mac-address-table aging-time

This command is used to configure the MAC address table ageing time. Use the **no** form of the 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.

Command Default Level

Level: 12.

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)#
```

40-3 mac-address-table aging destination-hit

This command is used to enable the destination MAC address triggered update function. Use the **no** form of the command to disable the destination MAC address triggered updated function.

mac-address-table aging destination-hit

no mac-address-table aging destination-hit

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The source MAC address triggered update function is always enabled. The hit bit of MAC address entries corresponding to the port that receives the packet will be updated based on the source MAC address and the VLAN of the packet. When the user enables the destination MAC address triggered update function by using the **mac-address-table aging destination-hit** command, the hit bit of MAC address entries corresponding to the port that transmit the packet will be updated based on the destination MAC address and the VLAN of the packet.

The destination MAC address triggered update function increases the MAC address entries hit bit update frequency and reduce traffic flooding by the MAC address entries aging time-out.

Example

This example shows how to enable the destination MAC address triggered update function.

```
Switch# configure terminal
Switch(config)# mac-address-table aging destination-hit
Switch(config)#
```

40-4 mac-address-table learning

This command is used to enable MAC address learning on the physical port. Use the **no** form of the command to disable learning.

mac-address-table learning interface *INTERFACE-ID* **[, | -]**

no mac-address-table learning interface *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	(Optional) Specifies the physical port interface to be configured.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this commands 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)#
```

40-5 mac-address-table notification change

This command is used to enable or configure the MAC address notification function. Use the **no** form of the command to disable the function or set the optional configuration to default.

mac-address-table notification change [interval *SECONDS* **| history-size** *VALUE***]**

no mac-address-table notification change [interval | history-size]

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.

Default

MAC address notification is disabled.

The default trap interval is 1 second.

The default number of entries in the history table is 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

40-6 mac-address-table static

This command is used to add a static address to the MAC address table. Use the **no** form of the 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 separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces are allowed before and 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

No static addresses are configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 the Ethernet interface 1/0/1.

```
Switch# configure terminal
Switch(config)# mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface eth1/0/1
Switch(config)#
```

This example shows how to add the static address C2:F3:22:0A:22:33 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:22:33 will be forwarded to port-channel 2.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/5-6
Switch(config-if-range)# channel-group 2 mode on
Switch(config-if-range)# exit
Switch(config)# mac-address-table static C2:F3:22:0A:22:33 vlan 4 interface port-
channel 2
Switch(config)#
```

40-7 multicast filtering-mode

This command is used to configure the handling method for multicast packets for a VLAN. Use the **no** form of the 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.

Command Default Level

Level: 12.

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)#
```

40-8 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 to display information for a specific interface. Valid

	interfaces include physical ports and port-channels.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID. The valid values are from 1 to 4094.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the option **interface** 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-C4-83     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#
```

40-9 show mac-address-table aging-time

This command is used to display the MAC address table's aging time.

show mac-address-table aging-time

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the MAC address table's aging time.

Example

This example shows how to display the MAC address table's aging time.

```
Switch# show mac-address-table aging-time

Aging Time is 300 seconds

Switch#
```

40-10 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-ID	(Optional) Specifies the interface to be display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the interface is not specified, all existing interfaces will be displayed.

Example

This example shows how to display the MAC address learning status on all physical ports 1 to 10.

```
Switch# show mac-address-table learning interface ethernet 1/0/1-10

Interface                State
-----------------------  --------
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#
```

40-11 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 interface to display.
history	(Optional) Specifies to display the MAC address notification change history.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If no option is specified, the global configuration will be displayed. Use the **interface** keyword to display information about all interfaces. If the interface ID is included, the specified interface will be displayed.

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

Switch#
```

This example shows how to display the MAC address notification global configuration.

```
Switch#show mac-address-table notification change

MAC Notification Change Feature: Disabled
Interval between Notification Traps: 1 seconds
Maximum Number of Entries Configured in History Table: 1
Current History Table Length: 0
MAC Notification Trap State: Disabled

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#
```

40-12 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

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#
```

40-13 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 the 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable 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)#
```

40-14 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 the command to return 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

The traps for both address addition and address removal are disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 interface eth1/0/2.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# snmp trap mac-notification change added
Switch(config-if)#
```

41. GARP VLAN Registration Protocol (GVRP) Commands

41-1 clear gvrp statistics

This command is used to clear the statistics for a GVRP port.

clear gvrp statistics {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear GVRP statistic counters associated with all interfaces.
interface *INTERFACE-ID* **[,|-]**	Specifies the interfaces. Specify a single interface, a range of interfaces separated by a hyphen, or a series of interfaces separated by comma.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear the GVRP counters.

Example

This example shows how to clear statistics for all interfaces.

```
Switch# clear gvrp statistics all
Switch#
```

41-2 gvrp global

This command is used to enable the GVRP function globally and use the **no** command to disable the GVRP function globally.

gvrp global

no gvrp global

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Administrators can enable the global GVRP state and individual port's GVRP state to start GVRP on the port.

Example

This example shows how to enable the GVRP protocol global state.

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

41-3 gvrp enable

This command is used to enable the GVRP function on a port. Use the **no** command to disable the GVRP function on a port.

gvrp enable

no gvrp enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for both physical ports and port-channel interface configuration. This command only takes effect for hybrid mode and trunk mode. This command does not take effect if the Layer 2 protocol tunnel is enabled for GVRP.

Example

This example shows how to enable the GVRP function on interface eth1/0/1.

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

41-4 gvrp advertise

This command is used to specify the VLAN that are allowed to be advertised by the GVRP protocol. Use the **no** command to disable the VLAN advertisement function.

gvrp advertise {all | [add | remove] *VLAN-ID* **[, | -]}**

no gvrp advertise

Parameters

all	Specifies that all VLANs are advertised on the interface.
add	(Optional) Specifies a VLAN or a list VLANs to be added to advertise the VLAN list.
remove	(Optional) Specifies a VLAN or a list VLANs to be removed from the advertised VLAN list.
VLAN-ID **[,|-]**	(Optional) Specified the advertise VLAN list or the VLAN list to be added to or removed from the advertise VLAN list. If the **add** or **remove** parameter is not specified, the specified VLAN list overwrites the advertise VLAN list. The range is 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No spaces are required before and after the comma.
-	(Optional) Specifies a range of VLANs. No spaces are required before and after the hyphen.

Default

By default, no VLANs are advertised.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for both physical ports and port-channel interface configuration. Administrators can use the **gvrp advertise** command to enable the specified VLANs' GVRP advertise function on the specified interface. The command only takes effect when GVRP is enabled. The command only takes effect for hybrid mode and trunk mode.

Example

This example shows how to enable the advertise function of VLAN 1000 on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# gvrp advertise 1000
Switch(config-if)#
```

41-5 gvrp vlan create

This command is used to enable dynamic VLAN creation. Use the **no** command to disable the dynamic VLAN creation function.

gvrp vlan create

no gvrp vlan create

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When dynamic VLAN creation is enabled, if a port has learned a new VLAN membership and the VLAN does not exist, the VLAN will be created automatically. Otherwise, the newly learned VLAN will not be created.

Example

This example shows how to enable the creation of dynamic VLANs registered with the GVRP protocol.

```
Switch# configure terminal
Switch(config)# gvrp vlan create
Switch(config)#
```

41-6 gvrp forbidden

This command is used to specify a port as being a forbidden member of the specified VLAN. Use the **no** command to remove the port as a forbidden member of all VLANs.

gvrp forbidden {all | [add | remove] *VLAN-ID* **[, | -]}**

no gvrp forbidden

Parameters

all	Specifies that all VLANs, except VLAN 1, are forbidden on the interface.
add	(Optional) Specifies a VLAN or a list of VLANs to be added to the forbidden VLAN list.
remove	(Optional) Specifies a VLAN or a list of VLANs to be removed from the forbidden VLAN list.
VLAN-ID **[,|-]**	(Optional) Specified the forbidden VLAN list. If the add or remove option is not specified, the specified VLAN list will overwrite the forbidden VLAN list. The range is 2 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No spaces are required before and after the

	comma.
-	(Optional) Specifies a range of VLANs. No spaces are required before and after the hyphen.

Default

No VLANs are forbidden.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for both physical ports and port-channel interface configuration. As a forbidden port of a VLAN, a port is forbidden from becoming a member port of the VLAN via the GVRP operation. The VLAN specified by the command does not need to exist.

This command only affects the GVRP operation. The setting only takes effect when GVRP is enabled. The command only takes effect for hybrid mode and trunk mode.

Example

This example shows how to configure the interface eth1/0/1 as a forbidden port of VLAN 1000 via the GVRP operation.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# gvrp forbidden 1000
Switch(config-if)#
```

41-7 gvrp timer

This command is used to configure the GVRP timer value on a port. Use the **no** form of the command to revert the timer to the default setting.

gvrp timer [join *TIMER-VALUE***] [leave** *TIMER-VALUE***] [leave-all** *TIMER-VALUE***]**

no gvrp timer [join] [leave] [leave-all]

Parameters

join	(Optional) Specifies to set the timer for joining a group. The unit is in a hundredth of a second.
leave	(Optional) Specifies to set the timer for leaving a group. The unit is in a hundredth of a second.
leave-all	(Optional) Specifies to set the timer for leaving all groups. The unit is in a hundredth of a second.
TIMER-VALUE	Specifies the timer value in a hundredth of a second. The valid range is 10 to 10000.

Default

Join: 20.

Leave: 60.

Leave-all: 1000.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the GVRP timer value on a port.

Example

This example shows how to configure the leave-all timer to 500 hundredths of a second on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# gvrp timer leave-all 500
Switch(config-if)#
```

41-8 gvrp nni-bpdu-address

This command is used to configure the GVRP BPDU address in the service provider site. Use the **no** form of the command to reset it to the default setting.

gvrp nni-bpdu-address {dot1d | dot1ad}

no gvrp nni-bpdu-address

Parameters

dot1d	Specifies to set the GVRP BPDU protocol address to 802.1d GVRP address 01:80:C2:00:00:21.
dot1ad	Specifies to set the GVRP BPDU protocol address to 802.1ad GVRP address 01:80:C2:00:00:0D.

Default

Dot1d GVRP address.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Generally, the GVRP BPDU address uses a Dot1d GVRP address. This command is used to designate the GVRP BPDU address as a Dot1d or Dot1ad GVRP address in the service provider site. It will only take effect on VLAN trunk ports that behave as the NNI ports in the service provider site.

Example

This example shows how to configure the GVRP PDU address in service provider site to dot1d.

```
Switch# configure terminal
Switch(config)# gvrp nni-bpdu-address dot1d
Switch(config)#
```

41-9 show gvrp configuration

This command is used to display the GVRP settings.

show gvrp configuration [interface [*INTERFACE-ID* **[,|-]]]**

Parameters

configuration	Specifies to display the GVRP configuration. If the interface is not specified, the GVRP global configuration is displayed.
interface	Specifies to display the GVRP interface configuration. If the interface ID is not specified, all interfaces are displayed.
INTERFACE-ID **[,|-]**	(Optional) Specifies the interfaces used to display the configuration. Specify a single interface or a range of interfaces, separated by a hyphen, or a series of interfaces separated by comma.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command only displays GVRP related configurations.

Example

This example shows how to display the GVRP configuration for the global configuration.

```
Switch# show gvrp configuration

Global GVRP State     : Enabled
Dynamic VLAN Creation : Disabled
NNI BPDU Address      : Dot1d

Switch#
```

This example shows how to display the GVRP configuration on interfaces eh3/0/5 to eth3/06.

```
Switch# show gvrp configuration interface eth3/0/5-3/0/6

eth3/0/5
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
```

```
Advertise VLAN  : 1-4094
Forbidden VLAN  : 3-5

eth3/0/6
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
Advertise VLAN  : 1-3
Forbidden VLAN  : 5-8

Switch#
```

41-10 show gvrp statistics

This command is used to display the statistics for a GVRP port.

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

Parameters

INTERFACE-ID **[,	-]**	(Optional) Specifies the interfaces. Specify a single interface, a range of interfaces separated by a hyphen, or a series of interfaces separated by commas.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command only displays the ports which have the GVRP state enabled.

Example

This example shows how to display statistics for GVRP interfaces eth3/0/5 to eth3/0/6.

```
Switch# show gvrp statistics interface eth3/0/5–3/0/6

Port        JoinEmpty       JoinIn  LeaveEmpty     LeaveIn   LeaveAll    Empty
----------- ----------- ----------- ----------- ---------- ----------- --------
eth3/0/5 RX          0             0           0          0          0          0
         TX 4294967296    4294967296  4294967296  4294967296 4294967296 4294967296
eth3/0/6 RX          0             0           0          0          0          0
         TX          0             0           0          0          0          0

Switch#
```

42. Gratuitous ARP Commands

42-1 ip arp gratuitous

This command is used to enable the learning of gratuitous ARP packets in the ARP cache table. To disable ARP control, use the **no** form of this command.

ip arp gratuitous

no ip arp gratuitous

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12,15.

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)#
```

42-2 ip gratuitous-arps

This command is used to enable the transmission of gratuitous ARP request packets. To disable the transmission, use the **no** form of this command.

ip gratuitous-arps [dad-reply]

no ip gratuitous-arps [dad-reply]

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

42-3 arp gratuitous-send

This command is used to set the interval for regularly sending of gratuitous ARP request messages on the interface. Use **no** 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 in the range from 1 to 3600 seconds.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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)#
```

43. IGMP Proxy Commands

43-1 ip igmp proxy

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

ip igmp proxy

no ip igmp proxy

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The IGMP proxy only works in a simple tree topology. Make sure that there are no other multicast routers except for the proxy devices in the simple tree topology. When receiving IGMP report packets from a downstream interface, IGMP proxy will update its membership database which is generated by the merger of all subscriptions on any downstream interface. If the database is changed, the proxy device will send unsolicited reports or leaves from upstream interface. It can also send membership reports from the upstream interface when queried.

Example

This example shows how to enable IGMP proxy on the device.

```
Switch# configure terminal
Switch(config)# ip igmp proxy
Switch(config)#
```

43-2 ip igmp proxy upstream

This command is used to configure an interface as the upstream in IGMP proxy. Use the **no** form of this command to disable the IGMP proxy upstream function on the interface.

ip igmp proxy upstream

no ip igmp proxy upstream

Parameters

None.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only one upstream can exist in an IGMP proxy device.

Example

This example shows how to configure interface VLAN 3 to act as the proxy upstream interface.

```
Switch# configure terminal
Switch(config)# interface vlan 3
Switch(config-if)# ip igmp proxy upstream
Switch(config-if)#
```

43-3 ip igmp proxy downstream

This command is used to configure an interface as a downstream in IGMP proxy. Use the **no** form of this command to disable the IGMP proxy downstream function on the interface.

ip igmp proxy downstream

no ip igmp proxy downstream

Parameters

None.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Multiple downstream interfaces can be configured on an IGMP proxy device.

Example

This example shows how to configure interface VLAN 4 to act as the proxy downstream interface.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if)# ip igmp proxy downstream
Switch(config-if)#
```

43-4 ip igmp proxy designated-forwarding

This command is used to enable designated forwarding on a non-querier IGMP proxy downstream interface. Use the **no** form of this command to disable it.

ip igmp proxy designated-forwarding

no ip igmp proxy designated-forwarding

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To avoid local loops and redundant traffic for links that are considered downstream links by multiple IGMP-based forwarders, IGMP proxy uses the IGMP querier election to elect a single forwarder on a LAN. Use this command to make a non-querier device a forwarder. Use the configuration in the appropriate topology. Improper usage may cause local loops or redundant traffic. The command does not take effect if the interface is not set as the downstream interface or set as the upstream interface.

Example

This example shows how to enable designated forwarding on downstream interface VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if)# ip igmp proxy designated-forwarding
Switch(config-if)#
```

43-5 show ip igmp proxy

This command is used to display IGMP proxy configurations.

show ip igmp proxy

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display upstream interface configurations and downstream interfaces.

Example

This example shows how to display the IGMP proxy configurations on the device.

```
Switch# show ip igmp proxy

IGMP Proxy Global State:    Enabled
Upstream Interface:          vlan14
Downstream Interface:
vlan11, vlan12(DF), vlan13(DF)

Switch#
```

43-6 show ip igmp proxy group

This command is used to display multicast groups learned by the IGMP proxy function.

show ip igmp proxy group [*GROUP-ADDRESS***]**

Parameters

GROUP-ADDRESS	Specifies the IPv4 multicast address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all group information by not specifying the group address.

Example

This example shows how to display the groups learned by IGMP proxy function.

```
Switch# show ip igmp proxy group

224.2.2.2, Exclude
Source list: 1.2.2.3, 1.3.3.8

227.3.1.5， Include
Source list: 3.2.3.9

Total entries: 2

Switch#
```

43-7 show ip igmp proxy forwarding

This command is used to display multicast forwarding entries created by the IGMP proxy function.

show ip igmp proxy forwarding [*GROUP-ADDRESS***]**

Parameters

GROUP-ADDRESS	Specifies the IPv4 multicast address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all proxy forwarding information by not specifying the group address.

Example

This example shows how to display the forwarding information created by the IGMP proxy function.

```
Switch# show ip igmp proxy forwarding

237.1.1.0, 100.52.1.10, vlan52
outgoing interface:
vlan20, vlan30

237.1.1.1, 100.52.1.10, vlan52
outgoing interface:
vlan20

Total Entries: 2

Switch#
```

44. IGMP Snooping Commands

44-1 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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#
```

44-2 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 VLAN interfaces.

The IGMP snooping global state is disabled by default.

Command Mode

Interface Configuration Mode.

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In the interface configuration mode, the command is only available for VLAN interface configuration. For a VLAN to operate with IGMP snooping, both the global state and per interface 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 operation on all VLANs.

```
Switch# configure terminal
Switch(config)# no ip igmp snooping
Switch(config)#
```

This example shows how to enable the IGMP snooping operation on VLANs that are IGMP snooping enabled.

```
Switch# configure terminal
Switch(config)# ip igmp snooping
Switch(config)#
```

This example shows how to disable IGMP snooping on a VLAN1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# no ip igmp snooping
Switch(config-vlan)#
```

44-3 ip igmp snooping access-group

This command is used to restrict the receivers on a subnet to only join the multicast groups that are permitted by a standard IP access list. To disable this function, use the **no** form of this command.

ip igmp snooping access-group *ACCESS-LIST-NAME* **[vlan** *VLAN-ID***]**

no ip igmp snooping access-group [vlan *VLAN-ID***]**

Parameters

ACCESS-LIST-NAME	Specifies a standard IP access list. To permit users to join a group (*, G), specify “any” in source address field and G in destination address field of the access list entry.
VLAN-ID	(Optional) Specifies a Layer 2 VLAN on a trunk port and applies the filter to packets arrive on that VLAN.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **ip igmp snooping access-group** command on the router to restrict the multicast traffic receiver to join to specific group. The destination address part of the access list represents the multicast group address that the receiver is permitted or denied to join.

Example

This example shows how to restrict the serviced IGMP snooping group for eth3/0/1 to group 226.1.1.1. In the following example, first, create an IP access list named “igmp_filter” which only permits the packets destined for group address 226.1.1.1. Then, associate this access group in interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# ip access-list igmp_filter
Switch(config-ip-acl)# permit any host 226.1.1.1
Switch(config-ip-acl)# end
Switch(config)# interface eth3/0/1
Switch(config-if)# ip igmp snooping access-group igmp_filter
Switch(config-if)#
```

This example shows how to restrict the serviced IGMP group for port-channel1 (which is on trunk mode) to group 226.1.1.1.

```
Switch# configure terminal
Switch(config)# interface port-channel 1
Switch(config-if)# ip igmp snooping access-group igmp_filter vlan 2
Switch(config-if)#
```

44-4 ip igmp snooping fast-leave

This command is used to configure IGMP Snooping fast-leave on the interface. Use the **no** form to disable the fast-leave option on the specified interface.

ip igmp snooping fast-leave

no ip igmp snooping fast-leave

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. The **ip igmp snooping fast-leave** command allows IGMP membership to be removed from a port right on 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)#
```

44-5 ip igmp snooping ignore-topology-change-notification

This command is used to make IGMP snooping to ignore STP changes and not to send an STP-triggered query on the interface. Use the **no** command to make IGMP snooping not to ignore STP changes and send an STP triggered query on the specified interface.

ip igmp snooping ignore-topology-change-notification

no ip igmp snooping ignore-topology-change-notification

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. An IGMP snooping switch is aware of link-layer topology changes caused by the Spanning Tree operation. When a port is enabled or disabled by the Spanning Tree, a General Query will be sent on all active non-router ports in order to reduce network convergence time. Use this command to make IGMP snooping ignore the topology change case.

Example

This example shows how to enable IGMP snooping ignoring topology change on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping ignore-topology-change-notification
Switch(config-vlan)#
```

44-6 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 the 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. On receiving an IGMP leave message, the IGMP snooping querier will assume that there are no local members on the interface 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)#
```

44-7 ip igmp snooping limit

This command is used to set the limitation on the number of IGMP cache entries that can be created. Use the **no** form of this command to remove the limitation

ip igmp snooping limit *NUMBER* **[exceed-action {drop | replace}] [except** *ACCESS-LIST-NAME***] [vlan** *VLAN-ID***]**

no ip igmp snooping limit [vlan *VLAN-ID***]**

Parameters

NUMBER	Specifies to set the maximum number of IGMP cache entries that can be created. This value must between 1 and 2048.
exceed-action	Specifies the action for handling newly learned groups when the

	limitation is exceeded. **drop:** Specifies that the new group will be dropped. **replace:** Specifies that the new group will replace the oldest group.
ACCESS-LIST-NAME	Specifies a standard IP access list. The group (*,G), or channel (S,G) permitted by the access list will be excluded from the limit. To permit a channel (S,G), specify S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specify “any” in the source address field and G in the destination address field of the access list entry.
VLAN-ID	(Optional) Specifies a Layer 2 VLAN on a trunk port and applies the filter to packets that arrive on that VLAN.

Default

By default, there is no limit.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for physical port or port-channel interface configuration. The except-option allows users to specify a standard access list to exclude a list of groups or channels from the limit. The **vlan** keyword option only takes effect on trunk ports. A system message will be generated and logged whenever the limit is exceeded.

Example

This example shows how to set the limit number of IGMP snooping groups that eth4/0/5 can join to.

```
Switch# configure terminal
Switch(config)# interface eth4/0/5
Switch(config-if)# ip igmp snooping limit 25 exceed-action drop
Switch(config-if)#
```

This example shows how to set the limit number of IGMP snooping groups that eth3/0/5 (which is a trunk port) can join to.

```
Switch# configure terminal
Switch(config)# interface eth3/0/5
Switch(config-if)# ip igmp snooping limit 100 vlan 2
Switch(config-if)#
```

This example shows how to set the limit number of IGMP snooping groups that eth4/0/3 (which is a hybrid port) can join to.

```
Switch# configure terminal
Switch(config)# interface eth4/0/3
Switch(config-if)# ip igmp snooping limit 100 vlan 3
Switch(config-if)#
```

This example shows how to set the limit number of IGMP snooping groups with a configuration limit from an ACL that eth4/0/24 (which is a trunk port) with the VLAN ID of 1000 can join to.

```
Switch# configure terminal
```

```
Switch(config)# interface eth4/0/24
Switch(config-if)# ip igmp snooping limit 80 except igmp_filter vlan 1000
Switch(config-if)#
```

This example shows how to set the limit number of IGMP snooping groups with a configuration limit from an ACL that port-channel 4 (which is an access port) with the VLAN ID of 100 can join to.

```
Switch# configure terminal
Switch(config)# interface port-channel4
Switch(config-if)# ip igmp snooping limit 55 except igmp_filter
Switch(config-if)#
```

This example shows how to reset the limit number to the default of IGMP snooping groups that port-channel 4 (which is a trunk port) with the VLAN ID of 1000 can join to.

```
Switch# configure terminal
Switch(config)# interface eth4/0/38
Switch(config-if)# no ip igmp snooping limit vlan 1000
Switch(config-if)#
```

This example shows how to reset the limit number to the default of IGMP snooping groups that port-channel 4 (which is a trunk port) can join.

```
Switch# configure terminal
Switch(config)# interface port-channel4
Switch(config-if)# no ip igmp anooping limit vlan 1
Switch(config-if)#
```

44-8 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	(Optional) Specifies an interface or an interface list. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces, or a separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

No IGMP snooping multicast router port is configured.

Auto-learning is enabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. 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. If auto-learn is disabled, the multicast router port can only be statically configured.

Example

This example shows how to add 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 eth4/0/1
Switch(config-vlan)#
```

44-9 ip igmp snooping proxy-reporting

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

ip igmp snooping proxy-reporting [source *IP-ADDRESS***]**

no ip igmp snooping proxy-reporting

Parameters

IP-ADDRESS	(Optional) Specifies the source IP of proxy reporting. The default value is zero IP.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. When the function proxy reporting is enabled, the received multiple IGMP report or leave packets for a specific (S, G) will be integrated into one report before being sent to the router port. Proxy reporting source IP will be used as source IP of the report, Zero IP address will be used when the proxy reporting source IP is not set. Interface MAC will be

used as source MAC of the report. If the VLAN has no IP address configured, then system MAC will be used.

Example

This example shows how to enable IGMP snooping proxy-reporting on VLAN 1 and configure the proxy-reporting message source IP to be 1.2.2.2.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-if)# ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-if)#
```

44-10 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. The interface must have IP address assigned to start the querier. The system will return warning message if the VLAN has no IP address. If querier is enabled, but IP address is removed, the querier will be stopped. 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. If IGMP protocol is also enabled on the interface, IGMP snooping querier state will be disabled automatically.

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)#
```

44-11 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 the 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. 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)#
```

44-12 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. This command configures the period of which the group member can respond to an IGMP query message before the IGMP Snooping deletes the membership.

Example

This example shows how to configure the maximum response time to 20 seconds on an interface.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping query-max-response-time 20
Switch(config-vlan)#
```

44-13 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 {1 | 2 | 3}

no ip igmp snooping query-version

Parameters

NUMBER	Specifies the version of the IGMP general query sent by the IGMP snooping querier.

Default

By default, this value is 3.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. 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 won't 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)#
```

44-14 ip igmp snooping rate-limit

This command is used to configure the upper limit per second for ingress IGMP control packets. Use the **no** form of this command to disable the rate limit.

ip igmp snooping rate-limit *NUMBER*

no ip igmp snooping rate-limit

Parameters

NUMBER	Specifies to configure the rate of the IGMP control packet that the switch can process on a specific interface. The rate is specified in packets per second.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for VLAN interface configuration, physical port or port-channel interface. The command configures the rate of IGMP control packet that can be processed by IGMP snooping.

Example

This example shows how to limit 30 packets per second on interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping rate-limit 30
Switch(config-vlan)#
```

44-15 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. 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)#
```

44-16 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 value.

ip igmp snooping robustness-variable *VALUE*

no ip igmp snooping robustness-variable

Parameters

VALUE	Specifies the robustness variable.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. 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 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 interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ip igmp snooping robustness-variable 3
Switch(config-vlan)#
```

44-17 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 a IP multicast group address.
INTERFACE-ID	(Optional) Specifies an interface or an interface list. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces, or a separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

By default, no static-group is configured.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. This command applies to IGMP snooping on a VLAN interface to statically add group membership entries and/or source records.

The **ip igmp snooping static-group** command allows the user 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 and source records for IGMP snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
```

```
Switch(config-vlan)# ip igmp snooping static-group 226.1.2.3 interface eth3/0/5
Switch(config-vlan)#
```

44-18 ip igmp snooping suppression-time

This command is used to configure the interval of suppressing duplicate IGMP reports or leaves. Use the **no** form of the 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 interval of suppressing duplicates IGMP reports. The range is from 1 to 300.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. The report suppression function will suppress the duplicate IGMP report or leave packets received in the suppression time interval. 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)#
```

44-19 ip igmp snooping minimum-version

This command is used to configure the minimum version of IGMP hosts that is allowed on the interface. Use the **no** form of this command to remove the restriction from the interface.

ip igmp snooping minimum-version {2 | 3}

no ip igmp snooping minimum-version

Parameters

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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. This setting only applies to the filtering of IGMP membership reports.

Example

This example shows how to restrict all IGMPv1 hosts to join.

```
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.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ip igmp snooping minimum version 3
Switch(config-vlan)#
```

This examples 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)#
```

44-20 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-ID	Specifies the VLAN to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 configurations.

```
Switch# show ip igmp snooping

IGMP snooping global state       : Enabled
Dynamic mrouter aging time       : 300 seconds

VLAN #1 Configuration
    IGMP snooping state             : Enabled
    Minimum version                 : v1
    Fast leave                      : Disabled (host-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
    Proxy reporting                 : Enabled (Source 1.2.3.4)
    Rate limit                      : 0
    Ignore topology change          : Disabled

Total Entries: 1

Switch#
```

44-21 show ip igmp snooping groups

This command is used to display IGMP snooping group information learned on the switch.

show ip igmp snooping groups [vlan *VLAN-ID* **[,|-] | [***IP-ADDRESS***]**

Parameters

vlan *VLAN-ID* **[,|-]**	(Optional) Specifies the VLAN interface to be displayed. If no VLAN is specified, IGMP snooping group information of all VLANs will be displayed, at which IGMP Snooping is enabled.
IP-ADDRESS	(Optional) Specifies the group IP address to be displayed. If no IP address is specified, all IGMP group information will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IGMP snooping group information.

Example

This example shows how to display IGMP snooping group information.

```
Switch# show ip igmp snooping groups

IGMP Snooping Connected Group Membership:

VLAN ID  Group address    Source address   FM  Exp(sec)  Interface
-------  ---------------  ---------------  --  --------  ---------
1        239.255.255.250         *         EX  382       2/0/7

Total Entries: 1

Switch#
```

44-22 show ip igmp snooping filter

This command is used to display IGMP snooping filter configuration information for all interfaces on the switch or for a specified interface.

show ip igmp snooping filter [interface *INTERFACE-ID* **[,|-]]**

Parameters

INTERFACE-ID **[,|-]**	(Optional) Specifies that the interface can be a physical interface or a port-channel. If no interface is specified, IGMP snooping filter information on all interface will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the IGMP snooping limit and access group information.

Example

This example shows how to display IGMP snooping filter information when no interface is specified.

```
Switch# show ip igmp snooping filter
```

```
eth3/0/1：
     Rate limit: 30pps
     Access group：igmp_filter
Groups/Channel Limit：25 (Exception List: igmp_filter, exceed-action: drop)

eth3/0/3：
     Rate limit: 20pps

     vlan1：
Access group：igmp_filter
Groups/Channel Limit：Not Configured
     vlan2：
Access group：Not Configured
Groups/Channel Limit：100 (exceed-action: replace)

port-channel4：
Rate limit： Not Configured
Access group：Not Configured
Groups/Channel Limit：Not Configured

Switch#
```

This example shows how to display filter information of eth3/0/3.

```
Switch# show ipv6 igmp snooping filter interface eth3/0/3

eth3/0/3：
     Rate limit: 30pps
Groups/Channel Limit：25 (Exception List: igmp_filter, exceed-action: replace)
     Vlan1：
Access group：igmp_filter
     Vlan2：
Access group：Not Configured

Switch#
```

44-23 show ip igmp snooping mrouter

This command is used to display IGMP snooping m-router information learned and configured on the switch.

show ip igmp snooping mrouter [vlan *VLAN-ID* **[,|-]]**

Parameters

vlan *VLAN-ID* **[,|-]**	(Optional) Specifies the VLAN. If no VLAN is specified, IGMP snooping information on all VLANs will be displayed of which IGMP snooping is

	enabled.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display dynamically learned or manually configured multicast router interfaces.

Example

This example shows how to display IGMP snooping m-router information.

```
Switch# show ip igmp snooping mrouter

VLAN     Ports
-------- ---------------------------------
1        eth3/0/4 (static), eth3/0/3 (static)
         eth3/0/6 (forbidden)
         eth4/0/2 (dynamic)
2        eth4/0/4 (static)
         eth4/0/3 (dynamic)

Total Entries: 2

Switch#
```

44-24 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 *INTERFACE-ID*	Specifies the interface to display port statistics counters.
vlan *VLAN-ID*	Specifies the VLAN ID to display VLAN statistics.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 1, Query 0
IGMPv2 Rx: Report 0, Query 0, Leave 0
IGMPv3 Rx: Report 0, Query 0
IGMPv1 Tx: Report 0, Query 0
IGMPv2 Tx: Report 0, Query 0, Leave 0
IGMPv3 Tx: Report 0, Query 0

Total Entries: 1

Switch#
```

45. Interface Commands

45-1 clear counters

This command is used to clear counters for a physical port interface.

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

Parameters

all	Specifies to clear counters for all interfaces.
INTERFACE-ID	Specifies the interface ID to clear the counter.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear counters for a physical port interface.

Example

This example shows how to clear the counters of interface eth1/0/1.

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

45-2 description

This command is used to add a description to an interface.

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.

Command Default Level

Level: 12.

Usage Guideline

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 interface eth 1/0/10.

```
Switch# configure terminal
Switch(config)# interface eth1/0/10
Switch(config-if)# description Physical Port 10
Switch(config-if)#
```

45-3 interface

This command is used to enter the interface configuration mode for a single interface. Use the **no** form of the 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 with no spaces in between.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enter the interface configuration mode for a specific interface. The interface ID is formed by the interface type and interface number with no spaces in between.

The following keywords can be used for the supported interface types:

- **ethernet** - Specifies the Ethernet switch port with all different media.
- **null** - Specifies the null interface.
- **loopback** - Specifies the software only interface which always stays in the up status.
- **vlan** - Specifies the VLAN interface.
- **port-channel** - Specifies the aggregated port-channel interface.
- **tunnel** - Specifies the virtual interface used for tunneling purposes.
- **mgmt** - Specifies the Ethernet interface used for the out-of-band management port.

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 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 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.

For a null interface, the null0 interface is supported and can't be removed.

For a loopback interface or a tunnel interface, the **interface** command is used to create the interface or modify the interface setting. Use the **no** form of the command to remove the interface.

Example

This example shows how to enter the interface configuration mode for the interface eth 2/0/5.

```
Switch# configure terminal
Switch(config)# interface eth2/0/5
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)#
```

This example shows how to add a loopback interface 2 and then enter its interface configuration mode.

```
Switch# configure terminal
Switch(config)# interface loopback2
Switch (config-if)#
```

This example shows how to remove loopback interface 2.

```
Switch# configure terminal
Switch(config)# no interface loopback2
Switch (config)#
```

45-4 interface range

This command is used to enter the interface range configuration mode for multiple interfaces.

interface range Ethernet *PORTLIST*

Parameters

Ethernet	Specifies that Ethernet ports will be used for this configuration.
PORTLIST	Enter the list of ports that will be used for this configuration here.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enters the interface configuration mode for the specified range of interfaces. Commands configured in the interface range mode, applies to interfaces in the range.

Example

This example shows how to enter the interface configuration mode for the range of ports 2/0/1 to 2/0/5: and port 3/0/3.

```
Switch# configure terminal
Switch(config)# interface range Ethernet 2/0/1-5, 3/0/3
Switch(config-if-range)#
```

45-5 show counters

This command is used to display interface information.

show counters [interface *INTERFACE-ID***]**

Parameters

INTERFACE-ID	Specifies that the interface can be a physical port or VLAN interfaces. If no interface is specified, counters of all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the statistic counters for an interface.

Example

This example shows how to display the counters for interface eth1/0/1.

```
Switch#show counter interface eth1/0/1
```

```
eth1/0/1 counters
 rxHCTotalPkts                    : 0
 txHCTotalPkts                    : 0
 rxHCUnicastPkts                  : 0
 txHCUnicastPkts                  : 0
 rxHCMulticastPkts                : 0
 txHCMulticastPkts                : 0
 rxHCBroadcastPkts                : 0
 txHCBroadcastPkts                : 0
 rxHCOctets                       : 0
 txHCOctets                       : 0
 rxHCPkt64Octets                  : 0
 rxHCPkt65to127Octets             : 0
 rxHCPkt128to255Octets            : 0
 rxHCPkt256to511Octets            : 0
 rxHCPkt512to1023Octets           : 0
 rxHCPkt1024to1518Octets          : 0
 rxHCPkt1519to1522Octets          : 0
 rxHCPkt1519to2047Octets          : 0
 rxHCPkt2048to4095Octets          : 0
 rxHCPkt4096to9216Octets          : 0
 txHCPkt64Octets                  : 0
 txHCPkt65to127Octets             : 0
 txHCPkt128to255Octets            : 0
 txHCPkt256to511Octets            : 0
 txHCPkt512to1023Octets           : 0
 txHCPkt1024to1518Octets          : 0
 txHCPkt1519to1522Octets          : 0
 txHCPkt1519to2047Octets          : 0
 txHCPkt2048to4095Octets          : 0
 txHCPkt4096to9216Octets          : 0

 rxCRCAlignErrors                 : 0
 rxUndersizedPkts                 : 0
 rxOversizedPkts                  : 0
 rxFragmentPkts                   : 0
 rxJabbers                        : 0
 rxSymbolErrors                   : 0
 rxDropPkts                       : 0

 txCollisions                     : 0
 ifInErrors                       : 0
 ifOutErrors                      : 0
 ifInDiscards                     : 0
 ifInUnknownProtos                : 0
 ifOutDiscards                    : 0
 txDelayExceededDiscards          : 0
 txCRC                            : 0

 dot3StatsAlignmentErrors         : 0
 dot3StatsFCSErrors               : 0
 dot3StatsSingleColFrames         : 0
 dot3StatsMultiColFrames          : 0
```

```
 dot3StatsSQETestErrors             : 0
 dot3StatsDeferredTransmisions      : 0
 dot3StatsLateCollisions            : 0
 dot3StatsExcessiveCollisions       : 0
 dot3StatsInternalMacTransmitErrors : 0
 dot3StatsCarrierSenseErrors        : 0
 dot3StatsFrameTooLongs             : 0
 dot3StatsInternalMacReceiveErrors  : 0

 linkChange                         : 0

Switch#
```

45-6 show interfaces

This command is used to display the interface information.

show interfaces [*INTERFACE-ID* **[- | ,]]**

Parameters

INTERFACE-ID	(Optional) Specifies that the interface can be a physical port, VLAN, loopback interface, or other.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If no interface was specified, all existing interfaces will be displayed.

Example

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

```
Switch# show interfaces vlan1

VLAN1 is enabled, link status is down
Interface type: VLAN
Interface description: VLAN 1 for MIS
MAC address: 08-00-01-22-00-00

Switch#
```

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

```
Switch# show interfaces loopback1
```

```
loopback1 is enabled, link status is up
Interface type: Loopback
Interface description: Loopback 1 for MIS

Switch#
```

This example shows how to display the NULL interface information for interface null0.

```
Switch# show interfaces null0

Null0 is enabled, link status is up
Interface type: Null
Interface description: Null0 for MIS

Switch#
```

This example shows how to display the interface information for eth1/0/1.

```
Switch# show interfaces eth1/0/1

eth1/0/1 is enabled, link status is up
  Interface type: 1000BaseTx
  Interface description: Physical Ethernet port 1/0/1
  MAC Address: 00-03-04-29-00-00
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: on, receive flow-control: on
  Send flow-control oper: on, receive flow-control oper: on
  Full-duplex, 1Gb/s
  Maximum transmit unit:1536 bytes
  RX rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 0, TX bytes: 0
  RX rate: 0 packets/sec, TX rate: 0
  RX packets: 0, TX packets: 0
  RX multicast: 0, RX broadcast: 0
  RX CRC error: 0, RX undersize: 0
  RX oversize: 0, RX fragment: 0
  RX jabber: 0, RX dropped Pkts: 0
  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#
```

This example shows how to display the interface information for management port 0.

```
Switch# show interfaces mgmt0

mgmt0 is enabled, link status is up
Interface type: Management port
Interface description: mgmt_ipif for MIS

Switch#
```

45-7 show interfaces counters

This command is used to display counters on specified interfaces.

show interfaces [*INTERFACE-ID* **[,|-]] counters [errors]**

Parameters

errors	(Optional) Specifies to display the error counters.
INTERFACE-ID	(Optional) Specifies that the interface can be a physical port or VLAN interfaces. If no interface is specified, the counters on all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command allows the user to display switch port statistics counters.

Example

This example shows how to display switch port RX counters on ports 1 to 8.

```
Switch#show interfaces ethernet 1/0/1-8 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 ethernet 2/0/1-8,3/0/1-4 counters errors

Port      Align-Err   Fcs-Err  Rcv-Err   Undersize  Xmit-Err  OutDiscard
--------- ---------- --------- --------  ---------- --------- -----------
eth2/0/1          0         0         0           0         0           0
eth2/0/2          0         0         0           0         0           0
eth2/0/3          0         0         0           0         0           0
eth2/0/4          0         0         0           0         0           0
eth2/0/5          0         0         0           0         0           0
eth2/0/6          0         0         0           0         0           0
eth2/0/7          0         0         0           0         0           0
eth2/0/8          0         0         0           0         0           0
eth3/0/1          0         0         0           0         0           0
eth3/0/2          0         0         0           0         0           0
eth3/0/3          0         0         0           0         0           0
eth3/0/4          0         0         0           0         0           0

Port          Single-Col Multi-Col  Late-Col    Excess-Col Carri-Sen  Runts
------------- ---------- ---------- ----------  ---------- ---------- ----------

eth2/0/1      0          0          0           0          0          0         0
eth2/0/2      0          0          0           0          0          0         0
eth2/0/3      0          0          0           0          0          0         0
eth2/0/4      0          0          0           0          0          0         0
eth2/0/5      0          0          0           0          0          0         0
eth2/0/6      0          0          0           0          0          0         0
eth2/0/7      0          0          0           0          0          0         0
eth2/0/8      0          0          0           0          0          0         0
eth3/0/1      0          0          0           0          0          0         0
```

```
eth3/0/2      0          0          0          0          0          0          0
eth3/0/3      0          0          0          0          0          0          0
eth3/0/4      0          0          0          0          0          0          0

Port          Giants     Symbol-Err SQETest-Err DeferredTx IntMacTx   IntMacRx
------------- ---------- ---------- ----------  ---------- ---------- ----------
eth2/0/1      0          0          0          0          0          0          0
eth2/0/2      0          0          0          0          0          0          0
eth2/0/3      0          0          0          0          0          0          0
eth2/0/4      0          0          0          0          0          0          0
eth2/0/5      0          0          0          0          0          0          0
eth2/0/6      0          0          0          0          0          0          0
eth2/0/7      0          0          0          0          0          0          0
eth2/0/8      0          0          0          0          0          0          0
eth3/0/1      0          0          0          0          0          0          0
eth3/0/2      0          0          0          0          0          0          0
eth3/0/3      0          0          0          0          0          0          0
eth3/0/4      0          0          0          0          0          0          0

Total Entries:12

Switch#
```

45-8 show interfaces status

This command is used to display the switch's port connection status.

show interfaces [*INTERFACE-ID* **[,|-]] status**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the connection status of all switch ports will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the switch's port connection status.

Example

This example shows how to display the switch's port connection status.

```
Switch# show interfaces ethernet 1/0/1-8,3/0/1-2 status

Port          Status       VLAN         Duplex  Speed          Type
```

```
------------ ------------ ------------ ------- -------------- -------------
eth1/0/1      not-connected 1            auto    auto           10GBASE-R
eth1/0/2      not-connected 1            auto    auto           10GBASE-R
eth1/0/3      not-connected 1            auto    auto           10GBASE-R
eth1/0/4      not-connected 1            auto    auto           10GBASE-R
eth1/0/5      not-connected 1            auto    auto           10GBASE-R
eth1/0/6      not-connected 1            auto    auto           10GBASE-R
eth1/0/7      not-connected 1            auto    auto           10GBASE-R
eth1/0/8      connected     trunk        a-full  a-10G          10GBASE-R
eth3/0/1      connected     2            a-full  a-1000         10GBASE-R
eth3/0/2      not-connected 1            auto    auto           10GBASE-R

Total Entries: 10

Switch#
```

45-9 show interfaces utilization

This command is used to display the switch's port utilization.

show interfaces [*INTERFACE-ID* **[,|-]] utilization**

Parameters

utilization	(Optional) Specifies to display the utilization information.
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the utilization of all physical port interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the switch's physical port utilization.

Example

This example shows how to display the switch's port utilization.

```
Switch# show interfaces utilization

Port        TX packets/sec  RX packets/sec   Utilization
----------- -------------   --------------   -----------
eth1/0/1      0               0                0
eth1/0/2      1488109         0                50
eth1/0/3      0               0                0
eth1/0/4      0               1488109          50
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#
```

45-10 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

auto-negotiation	Specifies to display detailed auto-negotiation information.
INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the auto-negotiation information on all physical port interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the auto-negotiation information.

Example

This example shows how to display auto-negotiation information.

```
Switch# show interfaces ethernet 1/1/1-1/1/2 auto-negotiation

eth1/1/1
 Auto Negotiation: Disabled

eth1/1/2
 Auto Negotiation: Enabled

 Remote Signaling: Not detected
 Configure Status: Configuring
 Capability Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full, 1000M_Full
 Capability Received Bits: -
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError
```

```
Switch#
```

45-11 shutdown

This command is used to disable an interface. Use the **no** form of the command to enable an interface.

shutdown

no shutdown

Parameters

None.

Default

By default, this option is no shutdown.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The Physical port, loopback, VLAN, tunnel, and management interfaces are valid for this 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 enter the shutdown command to disable the port state of interface port 1/0/1.

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

46. Internet Group Management Protocol (IGMP) Commands

46-1 clear ip igmp groups

This command is used to clear dynamic group member information obtained from the response messages in the IGMP buffer.

clear ip igmp groups {all | *IP-ADDRESS* **| interface** *INTERFACE-ID***}**

Parameters

all	Specifies to clear all group entries.
IP-ADDRESS	Specifies to clear the specified group entry.
Interface *INTERFACE-ID*	Specifies to clear the group entries learned on the interface.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The IGMP buffer includes a list that contains the dynamic multicast groups that the hosts in the direct subnet join. Use this command to clear the dynamic group information. To delete all the dynamic group entries from the IGMP buffer, use the **clear ip igmp groups all** command.

Example

This example shows how to clear all entries from the IGMP cache.

```
Switch# clear ip igmp groups all
Switch#
```

This example shows how to clear entries for the multicast group 224.0.255.1 from the IGMP cache.

```
Switch# clear ip igmp groups 224.0.255.1
Switch#
```

This example shows how to clear the IGMP group cache entries from a specific interface of the IGMP group cache.

```
Switch# clear ip igmp groups interface vlan1
Switch#
```

46-2 ip igmp ignore-subscriber-ip-check

This command is used to disable checking the subscriber's source IP when an IGMP report or leave message is received. Use the **no** form of this command to reset to the default setting.

ip igmp ignore-subscriber-ip-check

no ip igmp ignore-subscriber-ip-check

Parameters

None.

Default

By default, the switch will check the subscriber's source IP.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

By default, the IGMP report or leave messages received by the interface will be checked to determine whether its source IP is in the same network as the interface. If they are not in the same network, the message information won't be learned by the IGMP protocol.

Use the **ip igmp ignore-subscriber-ip-check** command to disable the source IP check. If the check is disabled, the IGMP report or leave message with any source IP will be processed by the IGMP protocol.

Example

This example shows how to disable the subscriber's source IP check on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip igmp ignore-subscriber-ip-check
Switch(config-if)#
```

46-3 ip igmp enable

This command is used to enable the IGMP protocol state. Use the **no** form of this command to disable the IGMP protocol state.

ip igmp enable

no ip igmp enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. This command only takes effect when the interface has IP address configured.

Example

This example shows how to enable IGMP on VLAN 1.

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

46-4 ip igmp last-member-query-interval

This command is used to configure the interval at which the router sends IGMP group-specific or group-source-specific (channel) query messages. Use the **no** form of the command to revert to the default setting.

ip igmp last-member-query-interval *SECONDS*

no ip igmp last-member-query-interval

Parameters

SECONDS	Specifies the interval at which IGMP group-specific host query messages are sent. The range is from 1 to 25.

Default

By default, this value is 1 second.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the router receives a leave message from a receiver to claim leave from a group or a channel, the router will send the group specific query or group-source specific query message to the receiver interface. The IGMP last-member query interval will be advertised in the query message and conveyed to the receiver. This command configures the period that the router will send the next group-specific query or group-source specific query message if there is no report from receiver for the specific group or specific channel. The router will retry for the last member query count. If there is no report messages received after the retry count, the interface will be removed the membership from the specific group or specific channel.

Example

This example shows how to configure the IGMP last member query interval value to 2 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
```

```
Switch(config-if)# ip igmp enable
Switch(config-if)# ip igmp last-member-query-interval 2
Switch(config-if)#
```

46-5 ip igmp query-interval

This command is used to configure the interval at which the router sends IGMP general query messages periodically. Use the **no** form of the command to revert to the default setting.

ip igmp query-interval *SECONDS*

no ip igmp query-interval

Parameters

SECONDS	Specifies to configure the interval at which the designated router sends IGMP general query messages. The range is from 1 to 31744.

Default

By default, this value is 125 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the IGMP group member query interval. The IGMP querier sends IGMP query messages at the interval specified by **ip igmp query-interval** command to discover the receivers attached to the interface interested in joining to multicast groups. Hosts respond to the query with IGMP report messages to indicate the multicast group they are interested to join the membership.

Example

This example shows how to enable IGMP and configure the IGMP query interval to 300 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp enable
Switch(config-if)# ip igmp query-interval 300
Switch(config-if)#
```

46-6 ip igmp query-max-response-time

This command is used to configure the maximum response time advertised in IGMP queries. Use the **no** form of the command to revert to the default setting.

ip igmp query-max-response-time *SECONDS*

no ip igmp query-max-response-time

Parameters

SECONDS	Specifies to configure the maximum response time, in seconds, advertised in IGMP queries. The range is form 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command configures the period of which the group member can respond to an IGMP query message before the router deletes the membership. The group membership lifetime is equal to the query interval times the robustness plus the maximum response time.

Example

This example shows how to configure the IGMP maximum query response time to 10 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp query-max-response-time 10
Switch(config-if)#
```

46-7 ip igmp robustness-variable

This command is used to configure the robustness variable used in IGMP. Use the **no** form of this command to revert to the default value.

ip igmp robustness-variable *VALUE*

no ip igmp robustness-variable

Parameters

VALUE	Specifies the robustness variable.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 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.

Example

This example shows how to configure the robustness variable to be 3 on interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp robustness-variable 3
Switch(config-if)#
```

46-8 ip igmp ssm-map enable

This command is used to enable the SSM mapping for IGMPv1 or IGMPv2 hosts. Use the **no** form of the command to disable the mapping.

ip igmp ssm-map enable

no ip igmp ssm-map enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable SSM mapping for groups in the configured SSM range. SSM mapping is only applied to received IGMPv1 or IGMPv2 membership report packets.

Example

This example shows how to enable the SSM mapping for IGMPv1 or IGMPv2 hosts.

```
Switch# configure terminal
Switch(config)# ip igmp ssm-map enable
Switch(config)#
```

46-9 ip igmp ssm-map static

This command is used to create a static SSM mapping entry for IGMPv1 or IGMPv2 hosts. Use the **no** form of the command to delete an entry.

ip igmp ssm-map static *ACCESS-LIST SOURCE-ADDRESS*

no ip igmp ssm-map static *ACCESS-LIST SOURCE-ADDRESS*

Parameters

ACCESS-LIST	Specifies a standard IP access list that contains the multicast groups to be mapped. To permit a group, specify “any” in source address field and specify the group address in destination address field of the access list entry.
SOURCE-ADDRESS	Specifies the source address to be associated with the group defined in the access list.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The deployment of source specific multicast (SSM) allows the network service provider to manage the IP multicast address easily.

When SSM is enabled, the last hop router will initiate to establish a source-based tree for the channel (S, G) on receiving a (S, G) INCLUDE mode request that falls in the SSM range from the attached IGMPv3 hosts.

There are cases that the attached host is IGMPv1 or IGMPv2 hosts which only issue (*, G) requests. With the SSM mapping, if the multicast group being requested that falls in the SSM range, the router is able to map the (*, G) to a (S, G) requests based on the group address to source address mapping defined by the **ip igmp ssm-map static** command. The router will then issue to establish the source-based tree for the mapped (S, G).

The command can be issued multiple times. A group address can be associated with multiple source addresses if it is defined in multiple access lists. If multiple associations exist, the router will issue to establish a (S, G) source-based tree for each S.

Example

This example shows how to configure the SSM group range, enable the SSM mapping, and configure the SSM mapping entry.

```
Switch# configure terminal
Switch(config)# ip access-list SSM-GROUP
Switch(config-ip-acl)# permit any 232.0.0.0 255.0.0.0
Switch(config-ip-acl)# exit
Switch(config)# ip pim ssm range SSM-GROUP
Switch(config)# ip igmp ssm-map enable
Switch(config)# ip access-list CHANNEL-1
Switch(config-ip-acl)# permit any 232.1.1.1 255.255.255.255
Switch(config-ip-acl)# exit
```

```
Switch(config)# ip access-list CHANNEL-2
Switch(config-ip-acl)# permit any 232.1.1.2 255.255.255.255
Switch(config-ip-acl)# exit
Switch(config)# ip igmp ssm-map static CHANNEL-1 10.1.1.1
Switch(config)# ip igmp ssm-map static CHANNEL-2 10.2.1.1
Switch(config)#
```

46-10 ip igmp static-group

This command is used to create a static membership on an interface for a group or a channel. Use the **no** form of the command to remove the membership.

ip igmp static-group *GROUP-ADDRESS*

no ip igmp static-group *GROUP-ADDRESS*

Parameters

GROUP-ADDRESS	Specifies the IP multicast group address.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command allows the user to create an IGMP static group in case that when the attached host does not support the IGMP protocol. Once configured, the group member entry is added to the IGMP cache.

Example

This example shows how to configure a static IGMP group entry on VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp static-group 238.1.1.2
Switch(config-if)#
```

46-11 ip igmp version

This command is used to change the IGMP version on the specified interface. Use the **no** form of the command to revert to the default setting.

ip igmp version {1 | 2 | 3}

no ip igmp version

Parameters

1	Specifies to configure the switch to run IGMP version 1.
2	Specifies to configure the switch to run IGMP version 2.
3	Specifies to configure the switch to run IGMP version 3.

Default

The default IGMP version is 3.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Different IGMP versions support different functions for multicast data routing to hosts. Some commands are only effective for IGMPv2 and IGMPv3.For example, if you change to version 1, then the setting configured by the **ip igmp query-max-response-time** command will not be effective.

Example

This example shows how to configure the IGMP version to 3.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ip igmp enable
Switch(config-if)# ip igmp version 3
Switch(config-if)#
```

46-12 show ip igmp groups

This command is used to display IGMP group information on an interface.

show ip igmp groups [*IP-ADDRESS* **| interface** *INTERFACE-ID***] [{detail | static}]**

Parameters

IP-ADDRESS	(Optional) Specifies Group IP address to be displayed. If no IP address is specified, all IGMP group information will be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the interface to be displayed. If no interface is specified, IGMP group information for all interfaces that are IGMP enabled will be displayed.
detail	(Optional) Specifies to display detailed information.
static	(Optional) Specifies to display the static group.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Select to display multicast group information for a specific group or for a specific interface.

Example

This example shows how to display IGMP group information in interface VLAN 1000.

```
Switch# show ip igmp groups interface vlan1000

Interface       Group Address   Uptime          Expire         Last Reporter
-----------------------------------------------------------------------
vlan1000         224.0.1.149    0DT00H00M09S  0DT00H04M15S   10.10.0.91

Total Entries: 1

Switch#
```

This example shows how to display IGMP group detailed information of group 224.1.1.1.

```
Switch# show ip igmp groups 224.1.1.1 detail

Interface      : vlan1000
Group          : 224.1.1.1
Uptime         : 0DT00H00M42S
Expires        : Stopped
Group mode     : Include
Last reporter  : 192.168.50.111

Group source list:
      Source Address    v3 Exp
    ----------------- ----------
      192.168.55.55     0DT00H03M38S
      192.168.10.55     0DT00H03M38S

    Total Source Entries: 2

Interface     : vlan2000
Group         : 224.1.1.1
Uptime        : 0DT00H00M42S
Expires       : 0DT00H03M38S
Group mode    : Exclude
Last reporter : 192.168.51.111
Source list is empty

Total Entries: 2

Switch#
```

Display Parameters

Uptime	The time elapsed since the entry has been created in the format of

	[n]DT[n]H[n]M[n]S.
Expires	The time that the entry will be removed if there is no refresh on the entry in the format of [n]DT[n]H[n]M[n]S. Stopped indicates that timing out of this entry is not determined by this expire timer. If the router is in Include mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to Exclude mode before it times out).
Group mode	**Include** or **Exclude**: The group mode is based on the type of membership reports that are received on the interface for the group.
Last reporter	The last host to report being a member of the multicast group.

46-13 show ip igmp interface

This command is used to display IGMP configuration information on an interface.

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

Parameters

INTERFACE-ID	(Optional) Specifies a single interface, a range of interface separated by a hyphen, or a series of interface separated by a comma. If no interface is specified, the switch displays IGMP information on all interfaces on which IGMP is enabled. Note that only VLAN interfaces can be specified.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IGMP configuration settings on interfaces.

Example

This example shows how to display IGMP configuration information about interface VLAN 1000.

```
Switch# show ip igmp interface vlan1000

VLAN 1000
  Version                          : 3
  IP Address/Netmask              : 10.50.95.90/8
  IGMP State                       : Enabled
  Querier                          : 10.50.95.90
  Query Interval                  : 125 seconds
  Query Maximum Response Time : 10 seconds
  Robustness Variable             : 3
  Last Member Query Interval   : 2 seconds
```

```
  Subscriber Source IP Check   : Enabled

Total Entries: 1

Switch#
```

Display Parameters

Version	The IGMP protocol version running on the interface.
Querier	The querier IP on the interface LAN.
Subscriber Source IP Check	This field specifies whether to ignore the source IP check on incoming IGMP packets from subscriber. **Enable** indicates not to ignore the source IP check. **Disable** indicates to ignore the source IP check.

46-14 show ip igmp ssm-mapping

This command is used to display the SSM mapping configuration

show ip igmp ssm-mapping [*GROUP-ADDRESS***]**

Parameters

GROUP-ADDRESS	Specifies the multicast group to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the SSM source address mapping for a specified multicast group.

Example

This example shows how to display SSM mapping configurations.

```
Switch# show ip igmp ssm-mapping

SSM mapping : Enabled

Switch#
```

This example shows how to display SSM mapping for group address 232.1.1.1.

```
Switch# show ip igmp ssm-mapping 232.1.1.1
```

```
SSM Mapping : Enabled

Group address: 232.1.1.1
Source address: 10.1.1.1

Switch#
```

Display Parameters

SSM Mapping	Enabled/Disabled: Indicates that the SSM mapping function is enabled or disabled.
Group address	The SSM group address.
Source address	The source address which will be used to transfer the (*, G) to a (S, G) requests.

47. IP Multicast (IPMC) Commands

47-1 clear ip multicast-statistics

This command is used to clear the multicast protocol packet statistics counters.

clear ip multicast-statistics [igmp] [pim] [dvmrp]

Parameters

igmp	(Optional) Specifies to clear IGMP packets counter.
pim	(Optional) Specifies to clear PIM packets counter.
dvmrp	(Optional) Specifies to clear DVMRP packets counter.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear the multicast protocol packet statistics counter on the switch. If no parameters are specified, all IP multicast protocol statistics counter are cleared.

Example

This example shows how to clear the multicast protocol packet statistics counter.

```
Switch# clear ip multicast-statistics
Switch#
```

47-2 ip multicast table-lookup-mode

This command is used to configure the IP multicast forwarding lookup mode. Use the **no** form of this command to configure the IP multicast forwarding lookup mode to the default value.

ip multicast table-lookup-mode {ip | mac}

no ip multicast table-lookup-mode

Parameters

ip	Specifies the multicast forwarding lookup based on the IP address.
mac	Specifies the multicast forwarding lookup based on the MAC address.

Default

By default, the IP option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the IP multicast forwarding lookup mode.

Example

This example shows how to configure the IP multicast forwarding lookup mode to MAC.

```
Switch# configure terminal
Switch(config)# ip multicast table-lookup-mode mac
Switch(config)#
```

47-3 ip multicast-routing

This command is used to enable IP multicast routing. Use the **no** form of this command to disable IP multicast routing.

ip multicast-routing

no ip multicast-routing

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When IP multicast routing is disabled, the system will stop routing multicast packets even though the multicast routing protocol is enabled.

Example

This example shows how to enable IP multicast routing.

```
Switch# configure terminal
Switch(config)# ip multicast-routing
Switch(config)#
```

47-4 ip mroute

This command is used to create a static multicast route (mroute). Use the **no** form of this command to delete the route.

ip mroute *SOURCE-ADDRESS MASK* **{***RPF-ADDRESS* **| null}**

no ip mroute {*SOURCE-ADDRESS MASK* **| all}**

Parameters

SOURCE-ADDRESS	Specifies the network address of the multicast source.
MASK	Specifies the network mask for the multicast source.
RPF-ADDRESS	Specifies the RPF neighbor's IP address to reach the network.
null	Specifies that the RPF check will always fail for multicast traffic is sent from this source network.
all	Specifies to delete all IP multicast static routes.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The PIM protocol does not have its own routing table but uses the unicast routing table to determine the reverse path forwarding interface to reach a network. Use this command to configure the static multicast route to specify the RPF address for a network. If **null** is specified, then the RPF check will always fail for the source network specified by the command. If the RPF address is specified for the route, a lookup in the routing table will be done to resolve the RPF interface.

Example

This example shows how to configure the multicast data source within a network number 192.168.6.0/24 to be accessible with the neighbor router 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip mroute 192.168.6.0 255.255.255.0 10.1.1.1
Switch(config)#
```

This example shows how to configure the multicast data source within a network number 192.168.8.0/24 to be discarded.

```
Switch# configure terminal
Switch(config)# ip mroute 192.168.8.0 255.255.255.0 null
Switch(config)#
```

This example shows how to remove a previously configured IP mroute entry of 192.168.8.0/24.

```
Switch#configure terminal
Switch(config)# no ip mroute 192.168.8.0 255.255.255.0
Switch(config)#
```

47-5 show ip multicast

This command is used to display multicast information of the system or any IP interface.

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

Parameters

INTERFACE-ID	(Optional) Specifies the interface name to display IP multicast information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IP multicast interface information. If the keyword interface is not specified, the global state of IP multicast routing will be displayed. If the keyword interface is specified but the interface ID is not specified, this command will display the information for all interfaces.

Example

This example shows how to display the global state of IP multicast routing.

```
Switch# show ip multicast

IP multicast-routing global state: Enabled

Table lookup mode: IP

Switch#
```

This example shows how to display IP multicast interface information.

```
Switch# show ip multicast interface

Interface Name  IP Address         Multicast Routing
--------------- ------------------ ------------------
vlan1           192.168.20.10/24   N/A

Total Entries: 1

Switch#
```

47-6 show ip mroute

This command is used to display the content of the IP multicast routing table

show ip mroute [{[*GROUP-ADDRESS* **[***SOURCE-ADDRESS***] | dense | sparse | dvmrp] | summary | static}]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IP address.
SOURCE-ADDRESS	Specifies the multicast source IP address.
summary	(Optional) Specifies to display an one-line, abbreviated summary of each entry in the IP multicast routing table.
sparse	(Optional) Specifies to display only the PIM-SM routes.
dense	(Optional) Specifies to display only the PIM-DM routes.
dvmrp	(Optional) Specifies to display only the DVMRP routes.
static	(Optional) Specifies to display the multicast static routes.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Display the content of the IP multicast table. The uptime timer describes the time that the entry has been created. The expires timer is a keep-alive timer of the multicast data stream. The expires timer value is based on either the PIM Sparse or Dense Mode. If multicast data continues to arrive at the device, the timer will refresh. If the network address is specified, the switch displays the entries with source addresses that match the specified address.

Example

This example shows how to display multicast route brief information.

```
Switch# show ip mroute summary

IP Multicast Routing Table: 2 entries
Flags: D – PIM-DM, S – PIM-SM, V – DVMRP
Timers: Uptime/Expires
(10.10.1.52, 224.0.1.3), vlan1, 0DT00H01M32S/0DT00H03M20S, Flags: D
(20.1.1.1, 228.10.2.1), vlan10, 0DT00H05M10S/0DT00H03M11S, Flags: S

Switch#
```

This example shows how to display multicast route entries.

```
Switch# show ip mroute

IP Multicast Routing Table
Flags: D - PIM-DM, S - PIM-SM, V - DVMRP, s - SSM Group, F - Register flag
       P - Pruned, R - (S, G) RPT-bit set, T - SPT-bit set
Outgoing interface flags: W - Assert winner
Timers: Uptime/Expires
(10.10.1.52, 224.0.1.3), 0DT05H29M15S/0DT00H02M59S, flags: ST
Incoming interface: vlan1, RPF neighbor: 10.3.4.5
Outgoing interface list:
```

```
vlan121, Forwarding 0DT00H01M23S/0DT00H03M34S
vlan125, Forwarding 0DT00H01M23S/null

(20.1.1.1, 228.0.0.20), 0DT05H29M15S/0DT00H02M59S  flags: D
Incoming interface: vlan10, RPF neighbor: 10.3.4.5
Outgoing interface list: NULL

Total Entries: 2

Switch#
```

This example shows how to display a multicast sparse mode route entry.

```
Switch# show ip mroute sparse

(10.10.1.52, 224.0.1.3), 0DT05H29M15S/0DT00H02M59S, flags: ST
Incoming interface: vlan1, RPF neighbor: 10.3.4.5
Outgoing interface list:
vlan126, Forwarding 0DT00H00M03S/0DT00H04M07S
vlan127, Forwarding 0DT00H00M03S/0DT00H04M11S

Total Entries: 1

Switch#
```

This example shows how to display the static configured multicast route.

```
Switch#  show ip mroute static

Mroute: 192.168.6.0/24, RPF neighbor: 10.1.1.1
Mroute: 192.168.7.0/24, RPF neighbor: 10.1.1.1
Mroute: 192.168.8.0/24, RPF neighbor: NULL

Total Entries: 3

Switch#
```

47-7 show ip mroute forwarding-cache

This command is used to display the content of 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 group IP address.
source-addr *SOURCE-ADDRESS*	(Optional) Specifies the multicast source IP address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Display the content of the IP multicast forwarding cache information. IP multicast forwarding cache is a summary table from the IP multicast route table, IGMP snooping group member table, and 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: 1/0/1, T2

(*,225.0.0.0) VLAN0070
Outgoing interface list: 1/0/1-1/0/2

(10.1.1.1, 239.0.0.1) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 3

Switch#
```

47-8 show ip rpf

This command is used to check Reverse Path Forwarding (RPF) information for a given unicast host address.

show ip rpf *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IP address to display.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays how the IP multicast routing performs RPF. Because the router can find RPF information from multiple routing tables (For example, the Unicast Routing Information Base, or static mroutes), the **show ip rpf** command displays the source from which the information is retrieved.

Example

This example shows how to display RPF information for the unicast host with the IP address of 20.1.1.3.

```
Switch# show ip rpf 20.1.1.3

RPF information for 20.1.1.3
RPF interface: vlan11
RPF type: unicast
Metric: 10

Switch#
```

This example shows how to display RPF information for the unicast host with the IP address of 1.3.3.3.

```
Switch# show ip rpf 1.3.3.3

RPF information for 1.3.3.3
RPF neighbor: 2.1.5.1
RPF type: static

Switch#
```

This example shows how to display RPF information for the unicast host with the IP address of 3.2.2.2.

```
Switch# show ip rpf 3.2.2.2

RPF information for 3.2.2.2
RPF interface: NULL
RPF type: static

Switch#
```

Display Parameters

RPF neighbor	The IP address of the upstream router to source. This field is optional if the neighbor does not exist.
RPF type	**unicast** – RPF information is obtained from the unicast routing table. **static** – RPF information is obtained from the static multicast route.
Metric	Indicates the unicast routing metric. This field is optional if the metric does not exist.

47-9 show ip multicast-statistics

This command is used to display the received and sent multicast packet statistics counters.

show ip multicast-statistics [igmp] [pim] [dvmrp] [interface [*INTERFACE-ID*]]

Parameters

INTERFACE-ID	(Optional) Specifies the interface name for which to display IP multicast statistics counter.
igmp	(Optional) Specifies to display both received and sent IGMP packets counter.
pim	(Optional) Specifies to display both received and sent PIM packets counter.
dvmrp	(Optional) Specifies to display both received and sent DVMRP packets counter.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the counters of both received and sent multicast protocol packets on the switch according to the message type.

Example

This example shows how to display the multicast protocol packets counter on the switch.

```
Switch# show ip multicast-statistics

IGMP Packets Counter
                          Received         Sent
    IGMP Query v1/v2/v3     0/0/0         0/0/0
    IGMP Report v1/v2/v3    0/0/0         0/0/0
    IGMP Leave                0              0
    Unknown IGMP              0              0

PIM Packets Counter
                      Received     Sent
    PIM Hello           0              0
    PIM Register        0              0
    PIM Register-Stop   0              0
    PIM Join/Prune      0              0
    PIM Bootstrap       0              0
    PIM Assert          0              0
    PIM Graft           0              0
    PIM Graft-Ack      0              0
    PIM C-RP-Adv       0              0
    PIM State Refresh  0              0
    Unknown PIM        0              0

DVMRP Packets Counter
                      Received     Sent
```

```
    DVMRP Probe          0              0
    DVMRP Report         0              0
    DVMRP Prune          0              0
    DVMRP Graft          0              0
    DVMRP Graft-Ack      0              0
    Unknown DVMRP        0              0

Switch#
```

48. IP Source Guard Commands

48-1 ip verify source vlan dhcp-snooping

This command is used to enable IP source guard for a port. Use the **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

The command is available for physical port and port channel 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 option **ip-mac** is not specified, the validation is based on the source IP address and VLAN check only.
- If the option **ip-mac** 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 for eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# ip verify source vlan dhcp-snooping
Switch(config-if)#
```

48-2 ip source binding

This command is used to create a static entry used for IP source guard. Use the **no** form of the 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-ID	Specifies the port that the valid host is connected.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces are allowed before and after the hyphen.

Default

No entries are configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create a static binding entry used for IP source guard checking. Use the **no** command to delete a static binding entry. The parameters specified for the command must exactly match the configured parameters to be deleted.

If the MAC address and the VLAN for the configured entry already exist, the existing binding entry is updated. The interface specified for the command can be a physical port or a port-channel interface.

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 interface eth3/0/10.

```
Switch# configure terminal
Switch(config)# ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface
eth3/0/10
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 interface eth3/0/10.

```
Switch# configure terminal
Switch(config)# no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface
eth3/0/10
Switch(config)#
```

48-3 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-ID	(Optional) Specifies to display the IP-source guard binding entry based on ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional)Specifies a range of interfaces. No spaces are allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 IP Source Guard binding entries without any parameters.

```
Switch# show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-01 10.1.1.10        infinite  static        100    eth3/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100    eth3/0/3

Total Entries: 2

Switch#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.10.

```
Switch# show ip source binding 10.1.1.10
```

```
MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------ ----- ----------
00-01-01-01-01-01 10.1.1.10        infinite  static       100    eth3/0/3

Total Entries: 1

Switch#
```

This example shows how to display IP Source Guard binding entries by IP address 10.1.1.11, MAC address 00-01-01-01-01-10, at VLAN 100 on interface eth3/0/3 and learning by DHCP snooping.

```
Switch# show ip source binding 10.1.1.10 00-01-01-01-01-10 dhcp-snooping vlan 100
interface eth3/0/3

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------ ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth3/0/3

Total Entries: 1

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.

48-4 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-ID	(Optional) Specifies a port or a range of ports to configure.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional)Specifies a range of interfaces. No spaces are allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 eth3/0/3

Interface  Filter-type  Filter-mode IP address       MAC address       VLAN
---------  -----------  ----------- ---------------  ----------------- -------
eth3/0/3       ip       active      10.1.1.1                           100
eth3/0/3       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 eth3/0/3

Interface  Filter-type  Filter-mode  IP address       MAC address       VLAN
---------  -----------  -----------  ---------------  ----------------- -------
eth3/0/3       ip-mac     active       10.1.1.10        00-01-01-01-01-01 100
eth3/0/3       ip-mac     active       10.1.1.11        00-01-01-01-01-10 101
eth3/0/3       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.

49. IP Tunnel Commands

49-1 interface tunnel

This command is used to create a tunnel and enter the interface configuration mode. Use the **no** command to remove a tunnel.

interface tunnel *TUNNEL-ID*

no interface tunnel *TUNNEL-ID*

Parameters

TUNNEL-ID	Specifies the ID of the tunnel to be added, removed or configured. The valid range is 0 to 9999.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a tunnel and enter the interface configuration mode.

Example

This example shows how to create a tunnel interface with ID 2 and enter the interface configuration mode.

```
Switch# configure terminal
Switch(config)# interface tunnel 2
Switch(config-if)#
```

49-2 tunnel source

This command is used to specify the source IPv4 address or IPv6 address for the tunnel interface. Use the **no** command to remove the configuration.

tunnel source {*IPV4-ADDRESS* **|** *IPV6-ADDRESS***}**

no tunnel source

Parameters

IPV4-ADDRESS	Specifies the source IPv4 address for the tunnel interface.
IPV6-ADDRESS	Specifies the source IPv6 address for the tunnel interface.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for tunnel interface configuration. Use these commands to configure the source IP address for a tunnel interface. Assign the source IPv4 address for both manual and automatic IPv6 over IPv4 tunnel.

For manually configured tunnels, the source IP and destination IP address pairs need to be unique. The system will match the IP tunnel header in the received tunnel packet against the source IP and destination IP address pair of tunnels to identify the tunnel interface on which the packet is received.

The source IPv4 address of ISATAP and 6to4 tunnels needs to be unique since the system will identify the received tunnel based on the destination IPv4 address of the received packet.

Example

This example shows how to specify the source IPv4 address for tunnel interface 2 as 10.0.0.1.

```
Switch# configure terminal
Switch(config)# interface tunnel 2
Switch(config-if)# tunnel source 10.0.0.1
Switch(config-if)#
```

This example shows how to specify the source IPv6 address for tunnel interface 2 as 1000::1.

```
Switch# configure terminal
Switch(config)# interface tunnel 2
Switch(config-if)# tunnel source 1000::1
Switch(config-if)#
```

49-3 tunnel destination

This command is used to specify the destination IPv4 address or IPv6 address for the tunnel interface. Use the **no** command to remove the destination address setting.

tunnel destination {*IPV4-ADDRESS* **|** *IPV6-ADDRESS***}**

no tunnel destination

Parameters

IPV4-ADDRESS	Specifies the destination IPv4 address for the tunnel interface.
IPV6-ADDRESS	Specifies the destination IPv6 address for the tunnel interface.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for tunnel interface configuration. Use this command to configure the destination IPv4 or IPv6 address for a tunnel interface. Assign the destination IPv4 address for a manually configured IPv6 over IPv4 tunnel. The **tunnel destination** command setting only takes effect for manual tunnel interfaces.

Example

This example shows how to specify the destination IPv4 address for the tunnel interface 2 as 10.0.0.100.

```
Switch# configure terminal
Switch(config)# interface tunnel 2
Switch(config-if)# tunnel destination 10.0.0.100
Switch(config-if)#
```

This example shows how to specify the destination IPv6 address for the tunnel interface 2 as 1000::2.

```
Switch# configure terminal
Switch(config)# interface tunnel 2
Switch(config-if)# tunnel destination 1000::2
Switch(config-if)#
```

49-4 tunnel mode

This command is used to define the type of the IPv6 tunnel interface.

tunnel mode {ipv6ip [6to4 | isatap] | gre {ip | ipv6}}

Parameters

6to4	Specifies that the interface is a 6to4 tunnel interface.
isatap	Specifies that the interface is an ISATAP tunnel interface.
gre ip	Specifies that the interface is a GRE tunnel interface. The deliver protocol is IPv4 protocol.
gre ipv6	Specifies that the interface is a GRE tunnel interface. The deliver protocol is IPv6 protocol.

Default

By default, this option is configured as IPv6 IP manual mode.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for tunnel interface configuration. The tunneling of IPv6 over IPv4 can be either manually configured or automatic. The user needs to specify the destination IPv4 address for the manual IPv6 over IPv4 tunnel, but not for the automatic tunnel. The destination IPv4 address of the tunnel

is dynamically and automatically determined. There are two types of automatic IPv6 over IPv4 tunnels: 6to4 and ISATAP.

The 6to4 tunnel is mainly used for IPv6 network to network, or host to network communication. The ISATAP tunnel is mainly used for IPv6 host to host communication. RA message advertisements are suppressed on tunnel interfaces. Only ISATAP interfaces can unsuppress the advertising of RA messages.

For packets that are forwarded to a 6to4 tunnel, the destination address of the packet must be a 6to4 address. The IPv4 address in the destination IPv6 address of the packet will be the destination IPv4 address for the tunneled packet.

An ISATAP IPv6 address is in the form of IPv6 prefix::5EFE: IPv4 address.

For packets that are forwarded to an ISATAP tunnel, the destination address of the packet must be an ISATAP address. The IPv4 address in the destination IPv6 address of the packet will be the destination IPv4 address for the tunneled packet.

Example

This example shows how to specify tunnel 2 as an IPv6 manual tunnel.

```
Switch# configure terminal
Switch(config)# interface tunnel 2
Switch(config-if)# tunnel mode ipv6ip
Switch(config-if)#
```

This example shows how to specify tunnel 3 as an IPv6 6to4 tunnel.

```
Switch# configure terminal
Switch(config)# interface tunnel 3
Switch(config-if)# tunnel mode ipv6ip 6to4
Switch(config-if)#
```

49-5 show interface

This command is used to display interface information.

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

Parameters

INTERFACE-ID	Specifies the interface to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If an interface is not specified, then all existing interfaces will be displayed.

Example

This example shows how to display information for tunnel 3.

```
Switch#show interface tunnel3

tunnel3 is enabled, link status is up
   Interface type is tunnel
   Interface Description:
   Tunnel mode is ipv6ip
   Tunnel source 20.0.0.3(VLAN1), destination 11.76.2.3
   Tunnel TTL is inherited from IPv6 hop limit
   IPv6 address 3ffe:22:33:44::55/64

Switch#
```

49-6 show ipv6 interface

This command is used to display IPv6 interface information.

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

Parameters

INTERFACE-ID	Specifies the interface that will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If an interface is not specified, then all existing interfaces will be displayed.

Example

This example shows how to display information for tunnel 0.

```
Switch # show ipv6 interface tunnel0

Tunnel is enabled, Link status is down
  Tunnel mode is ipv6ip isatap
  IPv6 is disabled,
  Global unicast address:
      3ffe:501:ffff:100:a01:2ff:fe39:1/64

Switch#
```

50. IP Utility Commands

50-1 ping

This command is used to diagnose basic network connectivity.

ping [vrf *VRF-NAME*] **{***IP-ADDRESS* **|** *IPV6-ADDRESS* **|** *HOST-NAME*} **[count** *TIMES*] **[timeout** *SECONDS*] **[source {***IP-ADDRESS* **|** *IPV6-ADDRESS*}]

Parameters

vrf *VRF-NAME*	Specifies the name of the routing forwarding instance.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
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

If the **count** parameter is not specified, the default is sending 5 count packets.

If the **timeout** parameter is not specified, the timeout value will be 1 second.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to verify the reachability, reliability, and delay of the path to the destination host. If neither the count or timeout value is specified, the only way to stop the ping is by pressing Ctrl-C.

Example

This example shows how to ping the host with IP address 172.50.71.123.

```
Switch# ping 172.50.71.123

Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms
Reply from 172.50.71.123, time<10ms

 Ping Statistics for 172.50.71.123
 Packets: Sent =6, Received =6, 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#
```

50-2 ping access-class

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

ping access-class *IP-ACL*

no ping access-class

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.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command specifies an access list to restrict the access via ping.

Example

This example shows how a standard IP access list is created and is specified as the access list to restrict access via ping. Only the host 226.1.1.1 is allowed to ping the switch.

```
Switch# configure terminal
Switch(config)# ip access-list ping-filter
Switch(config-ip-acl)# permit 226.1.1.1 0.0.0.0
Switch(config-ip-acl)# end
Switch# ping access-class ping-filter
Switch#
```

50-3 traceroute

This command is used to display a hop-by-hop path from the switch through an IP network to a specific destination host.

traceroute [vrf *VRF-NAME***] {***IP-ADDRESS* **|** *IPV6-ADDRESS* **|** *HOST-NAME***}] [probe** *NUMBER***] [timeout** *SECONDS***] [max-ttl** *TTL***] [port** *DEST-PORT***]**

Parameters

vrf *VRF-NAME*	Specifies the name of the routing forwarding instance.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
IPV6-ADDRESS	Specifies the IPv6 address of the system to discover.
HOST-NAME	Specifies the host name of the system to discover.
probe *NUMBER*	(Optional) Specifies the number of datagrams to send. The allowed range is from 1 to 9.
timeout *SECONDS*	(Optional) Specifies the response timeout value, in seconds.
max-ttl *TTL*	(Optional) Specifies the maximum TTL value for outgoing UDP datagrams. The maximum allowed range is from 1 to 60.
port *DEST-PORT*	(Optional) Specifies the base UDP destination port number used in outgoing datagrams. This value is incremented each time a datagram is sent. The allowed range for the destination port is from 3000 to 64900. Use this option in the unlikely event that the destination host is listening to a port in the default trace-route port range.

Default

By default, three 40-byte UDP datagrams with an Initial TTL of 1 is sent.

The maximum TTL is 30.

The timeout period is 5 seconds.

The destination base UDP port number is 33434.

The query number for each TTL is 3.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

To interrupt this command after the command has been issued, press Ctrl-C.

This command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. A trace-route starts by sending a UDP datagram to the destination host with the TTL field set to 1. If a router finds a TTL value of 1 or 0, it drops the datagram and sends back an ICMP time-exceeded message to the sender. The trace-route facility determines the address of the first hop by examining the source address field of the ICMP time-exceeded message.

To identify the next hop, trace-route again sends a UDP packet, but this time with a TTL value of 2. The first router decrements the TTL field by 1 and send the datagram to the next router. The second router

sees a TTL value of 1, discards the datagram, and returns the time-exceeded message to the source. This process continues until the TTL is incremented to a value large enough for the datagram to reach the destination host (or until the maximum TTL is reached).

To determine when a datagram has reached its destination, trace-route sets the UDP destination port in the datagram to a very large value that the destination host is unlikely to be using. When a host receives a datagram with an unrecognized port number, it sends an ICMP port unreachable error to the source. This message indicates to the trace-route facility that it has reached the destination.

Use the TOS option to see if different types of service cause routes changes.

Example

This example shows how to trace-route the host 172.50.71.123.

```
Switch# traceroute 172.50.71.123

<10 ms  172.50.71.123

Trace complete.

Switch#
```

This example shows how to trace-route to the host 172.50.71.123, but the router does not reply.

```
Switch# traceroute 172.50.71.123

  *      Request timed out.
  *      Request timed out.

Switch#
```

This example shows how to trace-route to the host 172.50.71.123, but the router replies that the destination is unreachable.

```
Switch# traceroute 172.50.71.123

<10 ms  Network Unreachable
<10 ms  Network Unreachable

Switch#
```

This example shows how to trace-route to the host with the IPv6 address 2001:238:f8a:77:7c10:41c0:6ddd:ecab.

```
Switch# traceroute 2001:238:f8a:77:7c10:41c0:6ddd:ecab

<10 ms 2001:238:f8a:77:7c10:41c0:6ddd:ecab

Trace complete.

Switch#
```

50-4 ip helper-address

This command is used to add a target address for the forwarding of UDP broadcast packets. Use the **no** form of the command to remove a forwarding target address.

ip helper-address *IP-ADDRESS*

no ip helper-address *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the target IP address for the forwarding of the UDP broadcast packet.

Default

No IP helper-address is configured.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for VLAN interface configuration. Use this command to control the forwarding of UDP broadcast packets. This command takes effect only when the received interface has an IP address assigned.

The system only forwards the packet that satisfies the following restriction.

- The destination MAC address must be a broadcast address.
- The destination IP address must be an all-one broadcast.
- The packets are IPv4 UDP packets.
- The IP TTL value must be greater than or equal to 2.

Example

This example shows how to configure the IP helper-address to 172.50.71.123 for VLAN 100.

```
Switch# configure terminal
Switch(config)# interface vlan 100
switch(config-if)# ip helper-address 172.50.71.123
switch(config-if)#
```

50-5 ip forward-protocol

This command is used to enable the forwarding of a specific UDP service type of packets. Use the **no** form of the command to disable forwarding of a specific UDP service type of packets.

ip forward-protocol udp [*PORT***]**

no ip forward-protocol udp [*PORT***]**

Parameters

PORT	(Optional) Specifies the destination port of the UDP service to be forwarded or not forwarded.

Default

Common used application protocols are enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The following is a listing of the commonly used application protocols that will be forwarded by default if the IP helper address is configured. If the command or the **no** form of the command is configured without specifying the port number, then the default ports are applied. BOOTP UDP port 67 and 68 cannot be specified as the packets are forwarded by DHCP relay. Default ports are:

- Trivial File Transfer Protocol (TFTP) port 69.
- Domain Naming System (DNS) port 53.
- Time service port 37.
- NetBIOS Name Server port 137.
- NetBIOS Datagram Server port 138.
- TACACS service port 49.
- IEN-116 Name Service port 42.

Example

This example shows how the IP helper address is configured to 172.50.71.123 for VLAN 100. IP helper forwarding of UDP port 53 (DNS) is disabled.

```
Switch# configure terminal
Switch(config)# interface vlan 100
switch(config-if)# ip helper-address 172.50.71.123
switch(config-if)# exit
switch(config)# no ip forward-protocol udp 53
```

51. IP-MAC-Port Binding (IMPB) Commands

51-1 clear ip ip-mac-port-binding violation

This command is used to clear IP-MAC-Port Binding (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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to delete the IMPB violation entry from the filtering database.

Example

This example shows how to clear the entry blocked on interface eth1/0/4.

```
Switch# clear ip ip-mac-port-binding violation interface eth1/0/4
Switch#
```

51-2 ip ip-mac-port-binding

This command is used to enable the IMPB access control for port interfaces. Use the **no** form of the command to disable the IMPB access control function.

ip ip-mac-port-binding [*MODE***]**

no ip ip-mac-port-binding

Parameters

MODE	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 the mode option is not specified, the **strict-mode** is used.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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 eth3/0/10.

```
Switch# configure terminal
Switch(config)# interface eth3/0/10
Switch(config-if)# ip ip-mac-port-binding strict
Switch(config-if)#
```

51-3 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 to display for the specified interface.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
violation	(Optional) Specifies to display the blocked entry.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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
------- --------- ------------------
eth3/0/3      1       01-00-0c-cc-cc-cc
eth3/0/3      1       01-80-c2-00-00-00
eth3/0/4      1       01-00-0c-cc-cc-cd
eth3/0/4      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
---------- ------------
eth3/0/1       Strict
eth3/0/2       Strict
eth3/0/3       Loose
eth3/0/4       Loose

Total Entries: 4

Switch#
```

52. IPMCv6 Commands

52-1 ipv6 multicast-routing

This command is used to enable IPv6 multicast routing. Use the **no** form of this command to disable IPv6 multicast routing.

ipv6 multicast-routing

no ipv6 multicast-routing

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When IPv6 multicast routing is disabled, the system will stop routing multicast packets even though the multicast routing protocol is enabled.

Example

This example shows how to enable IPv6 multicast routing.

```
Switch# configure terminal
Switch(Config)# ipv6 multicast-routing
Switch(Config)#
```

52-2 ipv6 mroute

This command is used to create a static IPv6 multicast route (mroute). Use the **no** form of this command to delete the route.

ipv6 mroute *IPV6-PREFIXIPREFIX-LENGTH* **{***RPF-IPV6ADDRESS* **|** *INTERFACE-ID RPF-IPV6ADDRESS* **| null}**

no ipv6 mroute {*IPV6-PREFIXIPREFIX-LENGTH* **| all}**

Parameters

IPV6-PREFIX	Specifies the network address of the multicast source.
PREFIX-LENGTH	Specifies the prefix length for the multicast source. A decimal value that indicates how many of the high-order contiguous bits of the address comprise the prefix (the network portion of the address). A slash mark must precede the decimal value.

RPF-IPV6ADDRESS	Specifies the IPv6 address of the next hop that can be used to reach the specified network.
INTERFACE-ID	Specifies the RPF interface for the route. The interface where the RPF neighbor IPv6 address is located is the RPF interface.
null	Specifies that if null is specified for the route, the RPF check result will always fail.
all	Specifies to delete all IPv6 multicast static routes.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The PIM protocol does not have its own routing table but use the unicast routing table to determine the reverse path forwarding interface to reach a network. The user can use the **ipv6 mroute** command to configure static multicast routes to specify the RPF address for a network.

Example

This example shows how to configure the static route for multicast RPF checks.

```
Switch# configure terminal
Switch(config)# ipv6 mroute 2000::/64 6::6
Switch(config)#
```

This example shows how to configure the multicast data source within a network number 2000::/64 to be discarded.

```
Switch# configure terminal
Switch(config)# ipv6 mroute 2000::/64 null
Switch(config)#
```

This example shows how to remove a previously configured IPv6 mroute entry of 2000::/64.

```
Switch# configure terminal
Switch(config)# no ipv6 mroute 2000::/64
Switch(config)#
```

52-3 show ipv6 multicast

This command is used to display basic multicast information of the IPv6 interface.

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

Parameters

INTERFACE-ID	(Optional) Specifies the interface name for which to display IPv6

	multicast information. If no specific interface ID is specified, all interface will be displayed. If the keyword **interface** is not specified, the state of IPv6 multicast routing will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the basic multicast information of the IPv6 interface or display the state of IPv6 multicast routing. If the interface ID is not specified, this command will display the information for all IPv6 interfaces.

Example

This example shows how to display the state of IPv6 multicast routing.

```
Switch# show ipv6 multicast

IPv6 multicast-routing global state: Enabled

Switch#
```

This example shows how to display IPv6 multicast interface information.

```
Switch# show ipv6 multicast interface

Interface  Owner Module
vlan100    PIM-SM
vlan200    PIM-SM

Total Entries: 2

Switch#
```

Display Parameters

Interface	The interface name of the interface.
Owner Module	Indicates whether the module is enabled on the interface. **PIM-SM:** PIM Sparse Mode is enabled on this interface.

52-4 show ipv6 mroute

This command is used to display the content of the IPv6 dynamic multicast routing table.

show ipv6 mroute [*GROUP-ADDRESS* **[***SOURCE-ADDRESS***] | summary]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IPv6 address.
SOURCE-ADDRESS	(Optional) Specifies the multicast source IPv6 address.
summary	(Optional) Specifies to display a one-line, abbreviated summary of each entry in the IPv6 multicast routing table.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the content of the IPv6 multicast table. The “Uptime” timer describes the time that the entry has been created. The “Expires” timer is the keep-alive timer of the multicast data stream. The expires timer value is based on the PIM Sparse-mode. If the multicast data continues to arrive on the device, this timer will refresh. If the network address is specified, the switch displays the entries with source addresses that match the specified address. If no optional keyword is specified, all dynamic multicast routes will be displayed.

Example

This example shows how to display multicast route brief information.

```
Switch# show ipv6 mroute summary

IPv6 Multicast Routing Table: 2 entries
Flags: S – Sparse
Timers: Uptime/Expires

(2000::1010:134, FF07::1), vlan1, 0DT00H01M32S/0DT00H03M20S, Flags: S
(2000::2001:101, FF06::100), vlan10, 0DT00H05M10S/0DT00H03M11S, Flags: S

Switch#
```

This example shows how to display multicast route entries.

```
Switch# show ipv6 mroute

IPv6 Multicast Routing Table – 2 entries
Flags: S – Sparse
Timers: Uptime/Expires
(2000::1010:0134, FF07::1), 0DT05H29M15S/0DT00H02M59S, Flags: S
Incoming interface: vlan1
RPF nbr: 2000::103:405
Outgoing interface list:
vlan2
vlan3
(2000::2001:0101, FF06::20), 0DT05H29M15S/0DT00H02M59S  Flags: S
Incoming interface: vlan10
RPF nbr: 2000::1003:405
Outgoing interface list:
```

```
  vlan20

Switch#
```

Display Parameters

Flags	Provides information about the entry. S – Sparse. Entry is operating in sparse mode.
Timers: Uptime/Expires	"Uptime" indicates per interface how long (in day, hours, minutes, and seconds) the entry has been in the IPv6 multicast routing table. "Expires" indicates per interface how long (in day, hours, minutes, and seconds) until the entry will be removed from the IPv6 multicast routing table
Incoming interface	Expected interface for a multicast packet from the source. If the packet is not received on this interface, it is discarded.
RPF nbr	The IPv6 address of the upstream router to the RP or source.
Outgoing interface	Interfaces through which packets will be forwarded. For (S,G) entries, this list will not include the interfaces inherited from the (*,G) entry.

52-5 show ipv6 mroute forwarding-cache

This command is used to display the content of 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 group IPv6 address.
source-addr *SOURCE-ADDRESS*	Specifies the multicast source IPv6 address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the content of the IPv6 multicast forwarding cache information. IPv6 multicast forwarding cache is a summary table from the IPv6 multicast route table, MLD snooping group member table, and 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: 1/0/1, T2

(2000:60:1:1::10, ff0e::1:1:2) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 2

Switch#
```

52-6 show ipv6 mroute static

This command is used to display IPv6 static multicast routes.

show ipv6 mroute static

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IPv6 static configured multicast routes.

Example

This example shows how to o display IPv6 static configured multicast routes.

```
Switch#  show ipv6 mroute static

Mroute: 2000:: /64
RPF nbr: 2000::1001:0101
Mroute: 2001:: /64
RPF nbr: 2000::1001:0101, interface: vlan10
Mroute: 2002:: /64
Interface: null

Total Entries: 3
Switch#
```

Display Parameters

RPF nbr	The IPv6 address of the upstream router to the RP or source.

Mroute	Indicates the IPv6 prefix of the remote network.
Interface	Specifies the interface of the next router (RPF neighbor) to the remote network.

52-7 show ipv6 rpf

This command is used to check Reverse Path Forwarding (RPF) information for a given unicast host address.

show ipv6 rpf *IPV6-ADDRESS*

Parameters

IPV6-ADDRESS	Specifies the IPv6 address to display.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays how IPv6 multicast routing performs RPF. Because the router can find RPF information from multiple routing tables (for example, Unicast Routing Information Base, or static mroutes), this command displays the source from which the information is retrieved.

Example

This example shows how to display RPF information for the unicast host with the IPv6 address of 2001::1:1:3.

```
Switch# show ipv6 rpf 2001::1:1:3

RPF information for 2001::1:1:3
RPF interface: vlan11
RPF neighbor: FE80::40:1:3
RPF route/mask: 2001::/64
RPF type: unicast
Metric: 2

Switch#
```

This example shows how to display RPF information for the unicast host with the IPv6 address of 2000::1000:3.

```
Switch# show ipv6 rpf 2000::1000:3

RPF information for 2000::1000:3
RPF neighbor: 2000::1001:0101
```

```
RPF route/mask: 2000::1000:0/64
RPF type: static

Switch#
```

This example shows how to display RPF information for the unicast host with the IPv6 address of 2000::3000:301.

```
Switch# show ipv6 rpf 2000::3000:301

RPF information for 2000::3000:301
RPF interface: vlan10
RPF neighbor: FE80::200:FF:FE26:666C
RPF route/mask: 3002::/64
RPF Type: static

Switch#
```

Display Parameters

RPF neighbor	The IPv6 address of the upstream router to the RP or source. This field is optional if the neighbor does not exist.
RPF type	unicast – RPF information is obtained from the unicast routing table. static – RPF information is obtained from the static multicast route.
Metric	Indicates the unicast routing metric. This field is optional if the metric does not exist.

53. IPv6 Snooping Commands

53-1 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** 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

53-2 protocol

This command is used to specify that addresses should be snooped with DHCPv6 or NDP. Use the **no** 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

Both DHCPv6 and ND snooping are disabled.

Command Mode

IPv6 Snooping Configuration Mode.

Command Default Level

Level: 12.

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)#
```

53-3 limit address-count

This command is used to limit the maximum number of IPv6 snooping binding entries. Use the **no** command to reset it to default.

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 1024.

Default

By default, there is no limit configured.

Command Mode

IPv6 Snooping Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

53-4 ipv6 snooping attach-policy

This command is used to apply an IPv6 snooping policy to a specified VLAN. Use the **no** 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

No IPv6 snooping policy is applied.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

After an IPv6 snooping policy has been created, use this command to apply the policy on a specific VLAN.

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)#
```

53-5 ipv6 snooping station-move deny

This command is used to deny the station move function for IPv6 snooping entries. Use the **no** command to reset it to default.

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.

Command Default Level

Level: 12.

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)#
```

53-6 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the policy name is specified, only the specified policy information is displayed.

If the policy name is not specified, information is displayed for all policies.

Example

This example shows how to display DHCPv6 guard information.

```
Switch# show ipv6 snooping policy
```

```
Snooping policy: test1
        Protocol: DHCP, NDP
        Limit Address Count: 30
        Target VLAN: 100,200-210,4000

Switch#
```

Display Parameters

Protocol	The protocol used for snooping.
Limit Address Count	The maximum number of this IPv6 Snooping policy.
Target VLAN	The name of the target. The target is a VLAN list.

54. IPv6 Source Guard Commands

54-1 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-ID	Specifies the binding VLAN of the manual binding entry.
IPV6-ADDRESS	Specifies the IPv6 address of the manual binding entry.
INTERFACE-ID	Specifies the interface number of the manual binding entry.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used 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 interface eth3.10.

```
Switch# configure terminal
Switch(config)# ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface
eth3/0/1
Switch(config)#
```

54-2 ipv6 source-guard policy

This command is used to create an IPv6 source guard policy. This command will 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.

Command Default Level

Level: 12.

Usage Guideline

The command is used to create 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)#
```

54-3 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 disabled.

Command Mode

Source-guard Policy Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used 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)#
```

54-4 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 disabled.

Command Mode

Source-guard Policy Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable 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)#
```

54-5 ipv6 source-guard attach-policy

This command is used to apply IPv6 source guard on an interface. Use the **no** form of the command to remove this source guard from the interface.

ipv6 source-guard attach-policy [*POLICY-NAME***]**

no ipv6 source-guard attach-policy

Parameters

POLICY-NAME	Specifies the name of the source guard policy.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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 neighbor 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 interface eth1/0/3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

54-6 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	Specifies the name of the source guard policy.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is used to display the IPv6 source guard policy configuration. If the policy name is not 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 dhcp guard policy

Policy Test configuration:
    permit link-local
    deny global-autoconf
    Target: eth2/0/3
```

```
Switch#
```

54-7 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-ID	(Optional) Specifies to displays the binding entries that match the specified VLAN.
INTERFACE-ID	(Optional) Specifies to displays the binding entries that match the specified interface number.
IPV6-ADDRESS	(Optional) Specifies to displays the binding entries that match the specified IPv6 address.
MAC-ADDRESS	(Optional) Specifies to displays the binding entries that match the specified MAC address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The command is used to display the entries of the binding table.

Example

This example shows how to display the specified 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 eth0/0         100  8850
S FE80::21D:71FF:FE99:4900  001D.7199.4900  eth0/1         100   N/A
N 2001:600::1                   AABB.CC01.F500 eth0/0          100  3181
D 2001:300::1                   AABB.CC01.F500 port-channel3 100  9559
D 2001:100::2                   AABB.CC01.F600 eth1/0          200  9196
D 2001:400::1                   001D.7199.4900 eth1/2          100  1568
S 2001:500::1                   000A.000B.000C eth2/13         300  N/A

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.

55. Jumbo Frame Commands

55-1 max-rcv-frame-size

This command is used to configure the maximum Ethernet frame size allowed. Use the **no** form of the 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.

Default

By default, this value is 1536 bytes.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical ports 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 4/0/1.

```
Switch# configure terminal
Switch(config)# interface eth4/0/1
Switch(config-if)# max-rcv-frame-size 6000
Switch(config-if)#
```

56. Layer 2 Protocol Tunnel (L2PT) Commands

56-1 clear l2protocol-tunnel counters

This command is used to clear the Layer 2 Protocol Tunnel (L2PT) statistics counters.

clear l2protocol-tunnel counters {all | interface *INTERFACE-ID***}**

Parameters

all	Specifies to clear counters for all interfaces.
interface *INTERFACE-ID*	Specifies the interface to clear counters.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear protocol tunnel counters for all interfaces or for the specified interface. Only the physical port and port-channel interface can be specified for the command.

Example

This example shows how to clear L2PT counters for all L2PT ports.

```
switch# clear l2protocol-tunnel counters all
switch#
```

56-2 l2protocol-tunnel

This command is used to enable the protocol tunneling for the specified protocols. To disable the protocol tunneling, use the **no** form of the command.

l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

no l2protocol-tunnel [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

Parameters

gvrp	(Optional) Specifies to enable tunneling for GARP VLAN Registration Protocol (GVRP) packets.
stp	(Optional) Specifies to enables tunneling for Spanning Tree Protocol (STP) packets.
01-00-0c-cc-cc-cc	(Optional) Specifies to tunnel the protocol packets with this destination DA.

01-00-0c-cc-cc-cd	(Optional) Specifies to tunnel the protocol packets with this destination DA.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to enable tunneling of the Layer 2 protocol packet. With protocol tunneling, the protocol operation information at the local site and the remote site can be exchanged through the service provider network. If the protocol type is not specified, the command enables tunneling of all types of protocol packets.

Configure the Layer 2 protocol tunnel for GVRP/STP on the port whether GVRP/STP is enabled or not. However, the protocol operation of GVRP/STP will not work on the port when the corresponding Layer 2 protocol tunnel for GVRP/STP is enabled.

When a Layer 2 protocol packet arrives at port which is enabled for protocol tunneling, the switch will classify the packet with the service VLAN and forward the packet to the service VLAN member ports. Generally, the packet is encapsulated and forwarded to the remote site via the trunk port. When forwarding a packet to the remote site via a trunk port, the tunneled packet will be tagged with service VLAN. The packet can also be forwarded to other ports at the local site which are enabled for protocol tunnel.

Normally, protocol tunneling encapsulates the protocol packet by replacing the destination MAC address of the packet with a vendor specific multicast address. However, if the port being forwarded is Layer 2 protocol tunnel enabled, then the destination MAC address of the protocol packet will not be overwritten.

At the remote site, the switch decapsulates the tunneled packet by restoring the vendor specific multicast address to the original PDU address and forward the packet to the customer network via the ports that are enabled for protocol tunnel.

If the port that is enabled for the Layer 2 protocol tunnel receives encapsulated packets, then the port will enter the error-disable state.

Example

This example shows how to enable a tunneling protocol for the STP protocol on an interface.

```
Switch# configure terminal
Switch(config)# interface ethernet 1
Switch(config-if)# l2protocol-tunnel stp

 WARNING: STP doesn't run when l2 protocol tunnel is enabled for the port.

Switch(config-if)#
```

56-3 l2protocol-tunnel cos

This command is used to specify the CoS value for tunneling of the protocol packets. Use the **no** form of the command to reset to the default setting.

l2protocol-tunnel cos *COS-VALUE*

no l2protocol-tunnel cos

Parameters

COS-VALUE	Specifies the CoS value. The values are from 0 to 7. 7 is the highest priority.

Default

By default, this value is 5.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When a Layer 2 protocol packet arrives at a port that is enabled for the Layer 2 protocol tunnel, the switch will encapsulate the packet with a service VLAN tag and rewrites the CoS with the value specified by this command.

Example

This example shows how to specify a CoS value for tunneling of the protocol packets.

```
Switch# configure terminal
Switch(config)# l2protocol-tunnel cos 7
Switch(config)#
```

56-4 l2protocol-tunnel drop-threshold

This command is used to specify the threshold in tunneling of the specified Layer 2 protocol packets received by a port before it is dropped. Use the **no** form of the command to reset to the default setting.

l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}] *PPS*

no l2protocol-tunnel drop-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

Parameters

gvrp	(Optional) Specifies GVRP packets.
stp	(Optional) Specifies STP packets.
01-00-0c-cc-cc-cc	(Optional) Specifies the protocol packets with this destination DA.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this destination DA.
PPS	Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets per second.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The tunneling of the Layer 2 protocol packets will consume CPU processing power when encapsulating, decapsulating and forwarding packets. Use this command to restrict the CPU processing bandwidth consumption by specifying a threshold in the tunneling of the specified Layer 2 protocol packets received by a port before it is dropped. When the threshold is exceeded, the excessive incoming packets are dropped.

If protocol type is not specified, the setting applies to all protocol types.

The **l2protocol-tunnel drop-threshold** command can be used together with the **l2protocol-tunnel shutdown-threshold** command to restrict the processing bandwidth. If the shutdown threshold is also configured on the interface, the drop-threshold value must be less than or equal to the shutdown-threshold value.

Example

This example shows how to configure the drop threshold for the STP protocol.

```
Switch# configure terminal
Switch(config)# l2protocol-tunnel drop-threshold stp 2000
Switch(config-if)#
```

56-5 l2protocol-tunnel global drop-threshold

This command is used to specify the maximum number of Layer 2 protocol packets that can be processed by the system per second. Use the **no** form of the command to reset to the default setting.

l2protocol-tunnel global drop-threshold *PPS*

no l2protocol-tunnel global drop-threshold

Parameters

PPS	Specifies the maximum rate of incoming Layer 2 protocol packets that can be tunneled. This value must be between 100 and 20000.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The tunneling of the Layer 2 protocol packets will consume CPU processing power in encapsulating, decapsulating, and forwarding of the packet. Use the command to restrict the CPU processing bandwidth consumed by specifying a threshold on the number of all Layer 2 protocol packets that can be processed

by the system. When the maximum number of packets is exceeded, the excessive protocol packets are dropped.

Use the **l2protocol-tunnel global drop-threshold** command and the **l2protocol-tunnel drop-threshold** command in the global configuration mode to leverage the bandwidth restriction.

Example

This example shows how to enable rate limiting globally.

```
Switch# configure terminal
Switch(config)# l2protocol-tunnel global drop-threshold 5000
Switch(config)#
```

56-6 l2protocol-tunnel shutdown-threshold

This command is used to specify a threshold in the tunneling of the specified Layer 2 protocol packets received by a port before the shutdown. Use the **no** form of the command to reset to the default setting.

l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}] *PACKETS*

no l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}]

Parameters

gvrp	(Optional) Specifies GVRP tunneling.
stp	(Optional) Specifies STP tunneling.
01-00-0c-cc-cc-cc	(Optional) Specifies the protocol packets with this destination DA.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this destination DA.
PACKETS	Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to restrict the CPU processing bandwidth consumption by specifying a threshold for tunneling of the specified Layer 2 protocol packets received the port. When the threshold is exceeded, the port is put in error-disabled state.

If protocol type is not specified, the setting applies to all protocol types.

The **l2protocol-tunnel shutdown-threshold** command can be used together with the **l2protocol-tunnel drop-threshold** command. If drop threshold is also configured on the interface, the shutdown-threshold value must be greater than or equal to the drop-threshold value.

Example

This example shows how to specify the maximum number of STP packets that can be processed on that interface in 1 second.

```
Switch# configure terminal
Switch(config)# interface ethernet 1
Switch(config-if)# l2protocol-tunnel shutdown-threshold stp 200
Switch(config-if)#
```

56-7 show l2protocol-tunnel

This command is used to display the protocols that are tunneled on an interface or on all interfaces.

show l2protocol-tunnel [interface *INTERFACE-ID***]**

Parameters

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

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the Layer 2 protocol tunnel related settings, status, and counters.

Example

This example shows how to display the protocols that are tunneled on all interfaces.

```
Switch# show l2protocol-tunnel

CoS for Encapsulated Packets            :5
Drop Threshold for Encapsulated Packets :0

Protocol             Drop Counter
-----------------    ------------
gvrp                 0
stp                  0
01-00-0c-cc-cc-cc    0
01-00-0c-cc-cc-cd    0

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
eth3/0/3   gvrp         -         2000      8          0          0
eth3/0/5   gvrp         -         2000      8          0          0
           stp          -         2000      1268       1100       0
           01000ccccccc -         2000      0          0          0
```

```
Switch#
```

57. Link Aggregation Control Protocol (LACP) Commands

57-1 channel-group

This command is used to assign an interface to a channel group. Use the **no** form of the 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 16.
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.

Command Default Level

Level: 12.

Usage Guideline

The command is 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 mode **on** is specified in the command, the channel group type is static. If the mode **active** or **passive** is specified in the command, 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 the command 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 the **no interface port-channel** command.

If the security function is enabled on a port, then this port cannot be specified as a channel group member.

Example

This example shows how to assign Ethernet interfaces 1/0/4 to 1/0/5 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  eth1/0/4-1/0/5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

57-2 lacp port-priority

This command is used to configure the port priority. Use the **no** form of the 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.

Command Default Level

Level: 12.

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 interfaces 1/0/4 to 1/0/5.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-1/0/5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

57-3 lacp timeout

This command is used to configure the LACP long or short timer. Use the **no** form of this command to return to the default value.

lacp timeout {short | long}

no lacp timeout

Parameters

short	Specifies that there will be 3 seconds before invalidating received LACPDU information and there will be 1 second between LACP PDU periodic transmissions when using Short Timeouts.
long	Specifies that there will be 90 seconds before invalidating received LACPDU information and there will be 30 seconds between LACP

	PDU periodic transmissions when using Long Timeouts

Default

By default, the LACP timeout mode is short.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port interface configuration.

Example

This example shows how to configure the port LACP timeout to long mode on Ethernet interface 1/0/1.

```
Switch# configure terminal
Switch(config)# interface  eth1/0/1
Switch(config-if)# lacp timeout long
Switch(config-if)#
```

57-4 lacp system-priority

This command is used to configure the system priority. Use the **no** form of the command to revert the system priority back to the default value.

lacp system-priority *PRIORITY*

no lacp system-priroity

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.

Command Default Level

Level: 12.

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)#
```

57-5 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. To reset the load distribution to the default settings, use the **no** form of this command.

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac | dst-l4-port | src-dst-l4-port | src-l4-port}

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.
dst-l4-port	Specifies that the switch should examine the Layer 4 destination TCP/UDP port.
src-dst-l4-port	Specifies that the switch should examine the Layer 4 source TCP/UDP port and Layer 4 destination port
src-l4-port	Specifies that the switch should examine the Layer 4 source TCP/UDP port.

Default

The default load balance algorithm is **src-dst-mac**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

57-6 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-NO	(Optional) Specifies the channel group ID.
channel	(Optional) Specifies to display information for the specified port-channels.
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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If a port-channel number is not specified, all port-channels will be displayed. If the channel, **load-balance** and **sys-id** keywords are not specified with the **show channel-group** command, only summary channel-group information 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 = 12, Protocol: LACP
                     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 = 12, Protocol: Static
                     LACP         Port       Port
Port          Flags   State       Priority   Number
-----------------------------------------------
eth3/0/8      N/A      bndl       N/A        N/A
eth3/0/9      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 LACPDUs,
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   32768,00-07-eb-49-5e-80     12       SP        32768
eth1/0/2   32768,00-07-eb-49-5e-80     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: 32765,00-02-4b-29-3a-00
```

```
Group          Protocol
-------------------------
1               LACP
2               Static

Switch#
```

58. Link Layer Discovery Protocol (LLDP) Commands

58-1 clear lldp counters

This command is used to delete LLDP statistics.

clear lldp counters [all | interface *INTERFACE-ID* **[, | -]]**

Parameters

all	Specifies to clear LLDP counter information for all interfaces and global LLDP statistics.
interface *INTERFACE-ID*	Specifies the interface to clear LLDP counter information.
,	(Optional) Specifies a series of physical interfaces. No spaces before and after the comma.
-	(Optional) Specifies a range of physical interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command with the **interface** keyword to reset LLDP statistics of the specified interface(s). If the command **clear lldp counters** is issued with the **all** keyword to clear global LLDP statistics and the LLDP statistics on all interfaces. When no optional keyword is selected, only the LLDP global counters will be cleared.

Example

This example shows how to clear all LLDP statistics.

```
Switch# clear lldp counters all
Switch#
```

58-2 clear lldp table

This command is used to delete all 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-ID	Specifies the interface's ID.
,	(Optional) Specifies a series of physical interfaces. No spaces before and after the comma.
-	(Optional) Specifies a range of physical interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If this command is issued without the **interface** keyword, all neighboring information on all interfaces will be cleared.

Example

This example shows how to clear all neighboring information on all interfaces.

```
Switch# clear lldp table all
Switch#
```

58-3 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. To disable the transmission of TLVs, use the **no** form of this command.

lldp dot1-tlv-select {port-vlan | protocol-vlan *VLAN-ID* **[, | -] | vlan-name [***VLAN-ID* **[, | -]] | protocol-identity [***PROTOCOL-NAME***]}**

no lldp dot1-tlv-select {port-vlan | protocol-vlan [*VLAN-ID* **[, | -]] | 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's VLAN identifier (PVID) that will be associated with untagged or priority tagged frames.
protocol-vlan	Specifies the Port and Protocol VLAN ID (PPVID) TLV to send. The PPVID TLV is an optional TLV that allows a bridge port to advertise a port and protocol VLAN ID.
VLAN-ID **[,	-]**	Specifies the ID of the VLAN in the PPVID TLV. The VLAN ID range is 1 to 4094. Separate nonconsecutive VLAN IDs with a comma. Use a hyphen to designate a range of VLAN IDs. In the **no** form of this command, the VLAN ID is optional. If no VLAN ID is specified, all configured PPVID VLANs will be cleared and no PPVID TLV will be

	sent.
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 **[, | -]**	(Optional) Specifies the ID of the VLAN in the VLAN name TLV. The VLAN ID range is 1 to 4094. Separate nonconsecutive VLAN ID with a comma. Use a hyphen to designate a range of VLAN IDs. If no VLAN ID is specified, all applicable VLANs will be sent. In the **no** form of this command, 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.
protocol-identity [*PROTOCOL-NAME***]**	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. The valid strings for *PROTOCOL-NAME* are: **eapol:** Extensible Authentication Protocol (EAP) over LAN **lacp:** Link Aggregation Control Protocol **gvrp:** GARP VLAN Registration Protocol **stp:** Spanning Tree Protocol The protocol name is optional. When no specific protocol string is specified, all protocols are selected or de-selected in the **no** form of the command.

Default

No IEEE 802.1 Organizationally Specific TLV is selected.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port configurations. 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 configured VLAN ID matches the configuration of the protocol VLAN on that interface and the VLAN exists, then the PPVID TLV for that VLAN will be sent. 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 ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select port-vlan
Switch(config-if)#
```

This example shows how to enable advertising Port and Protocol VLAN ID TLV. The advertised VLAN includes 1 to 3.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-vlan 1-3
Switch(config-if)#
```

This example shows how to enable the VLAN Name TLV advertisement from vlan1 to vlan3.

```
Switch# configure terminal
Switch(config)#interface ethernet 1/0/1
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 ethernet 1/0/1
Switch(config-if)# lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

58-4 lldp dot1-tlv-select dcbx

This command is used to specify which optional type-length-value settings (TLVs) in the Data Center Bridging Exchange protocol (DCBX) TLV set will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. To disable the transmission of TLVs, use the **no** form of this command.

lldp dot1-tlv-select dcbx [ets-configuration | ets-recommendation | pfc-configuration]

no lldp dot1-tlv-select dcbx [ets-configuration | ets-recommendation | pfc-configuration]

Parameters

ets-configuration	(Optional) Specifies the Enhanced Transmission Selection Configuration TLV to send. The Enhanced Transmission Selection Configuration TLV is an optional TLV that allows a bridge port to advertise the current ETS operational state and willing bit.
ets-recommendation	(Optional) Specifies the Enhanced Transmission Selection Recommendation TLV to send. The Enhanced Transmission Selection Recommendation TLV is an optional TLV that allows a bridge port to advertise the ETS recommendation for the operational state of the remote port.
pfc-configuration	(Optional) Specifies the Priority-based Flow Control Configuration TLV to send. The Priority-based Flow Control TLV is an optional TLV that allows a bridge port to advertise the PFC current operational state and willing bit.

Default

By default, no DCBX TLV is selected and the DCBX state machine is enabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the optional TLVs advertisement state is enabled, they will be encapsulated in LLDPDU and sent to other devices.

The Data Center Bridging Exchange protocol (DCBX) is used by DCB devices to exchange configuration information with directly connected peers. The protocol may also be used for misconfiguration detection and for the configuration of the peer.

DCB exchanged attributes are packaged into organizationally specific TLVs. The OUI used for the DCBX TLV is the IEEE 802.1 OUI.

DCBX is expected to operate over a point-to-point link. If multiple LLDP peer ports running DCBX are detected, then DCBX should behave as if the peer port's DCBX TLVs are not present until the multiple LLDP peer port condition is no longer present. However, a transition in the LLDP peer port may occur in some circumstances (like a transition from the system boot to the system operation). Therefore when it is detected that the number of peer ports running DCBX exceeds 1 for a period longer than the longest TTL of any of the peers, a multi-peer condition is detected. During the time when the multi-peer condition has not been detected the DCBX data from the most recent DCBX peer will be used. An LLDP peer port is identified by a concatenation of the chassis ID and port ID values transmitted in the LLDPDU. A DCBX peer port is a LLDP peer port that is sending DCBX TLVs.

If ETS or PFC is disabled, the corresponding TLV won't be sent even if the corresponding TLV is selected.

Example

This example shows how to disable the Priority-based Flow Control TLV advertisement.

```
Switch# configure terminal
Switch(config)# no lldp dot1-tlv-select dcbx pfc-configuration
Switch(config-if)#
```

58-5 lldp dot3-tlv-select

This command is used to specify which optional type-length-value settings (TLVs) in the IEEE 802.3 Organizationally Specific TLV set will encapsulated in the LLDPDUs and sent to neighbor devices. To disable the transmission of the TLVs, use the **no** form of this command.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size | energy-efficient-eth]

no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | max-frame-size | energy-efficient-eth]

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 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.
energy-efficient-eth	(Optional) Specifies the energy efficient Ethernet TLV to send

Default

No IEEE 802.3 Organizationally Specific TLV is selected.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port configuration. This command enables 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 ethernet 1/0/1
Switch(config-if)# lldp dot3-tlv-select mac-phy-config
Switch(config-if)#
```

58-6 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 return to the default settings.

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.

Command Default Level

Level: 12.

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)#
```

58-7 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 return to the default settings.

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.

Command Default Level

Level: 12.

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)#
```

58-8 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.

Command Default Level

Level:12.

Usage Guideline

This command is available for physical port 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, then the address will not be sent.

When no optional address is specified along with the command **lldp management-address**, 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, then 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 enable eth3/0/1 and eth3/0/2 for setting the management address entry (IPv4).

```
Switch# configure terminal
Switch(config)# interface range eth3/0/1-3/0/2
Switch(config-if-range)# lldp management-address 10.1.1.1
Switch(config-if-range)#
```

This example shows how to enable eth3/0/3 and eth3/0/4 for setting the management address entry (IPv6).

```
Switch# configure terminal
Switch(config)# interface range eth3/0/3-3/0/4
Switch(config-if-range)# lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

This example shows how to delete the management address 10.1.1.1 from eth3/0/1 and eth3/0/2. If 10.1.1.1 is the last one, no Management Address TLV will be sent.

```
Switch# configure terminal
Switch(config)# interface range eth3/0/1-3/0/2
Switch(config-if-range)# no lldp management-address 10.1.1.1
```

```
Switch(config-if-range)#
```

This example shows how to delete the management address FE80::250:A2FF:FEBF:A056 from eth3/0/3. and eth3/0/4.

```
Switch# configure terminal
Switch(config)# interface range eth3/0/3-3/0/4
Switch(config-if-range)# no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

This example shows how to delete all management addresses from eth3/0/5 and then no Management Address TLV will be sent on eth3/0/5.

```
Switch# configure terminal
Switch(config)# interface eth3/0/5
Switch(config-if)# no lldp management-address
Switch(config-if)#
```

58-9 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. To disable the transmission of the TLVs, use the **no** form of this command.

lldp med-tlv-select [capabilities | inventory-management]

no lldp med-tlv-select [capabilities | inventory-management]

Parameters

capabilities	(Optional) Specifies to transmit the LLDP-MED capabilities TLV.
inventory-management	(Optional) Specifies to transmit the LLDP-MED inventory management TLV.

Default

No LLDP-MED TLV is selected.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port configuration. This command is used 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 ethernet 1/0/1
Switch(config-if)# lldp med-tlv-select capabilities
Switch(config-if)#
```

58-10 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.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port configuration. This command is used to enable a physical interface to receive LLDP messages. When LLDP is not running, the switch doesn't receive LLDP messages.

Example

This example shows how to enable a physical interface to receive LLDP messages.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp receive
Switch(config-if)#
```

58-11 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 return to the default settings.

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.

Command Default Level

Level: 12.

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)#
```

58-12 lldp run

This command is used to enable the Link Layer Discovery Protocol (LLDP) globally. Use the **no** form of this command to return to the default settings.

lldp run

no lldp run

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

58-13 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.

Command Default Level

Level: 12.

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)#
```

58-14 lldp tlv-select

This command is used to select the Type-Length-Value (TLVs) in the 802.1AB basic management set and will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. To disable this option, use the **no** form of this command.

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.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port configuration. This command is used 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 ethernet 1/0/1
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 ethernet 1/0/1
Switch(config-if)# lldp tlv-select system-name
Switch(config-if)#
```

58-15 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

LLDP transmit is enabled on all supported interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port configuration. This command is used to enable LLDP transmission on a physical interface. When LLDP is not running, the switch doesn't transmit LLDP messages.

Example

This example shows how to enable LLDP transmission.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# lldp transmit
Switch(config-if)#
```

58-16 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 return to the default settings.

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.

Command Default Level

Level: 12.

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)#
```

58-17 lldp tx-interval

This command is used to configure the LLDPDUs transmission interval on the switch. Use the **no** form of this command to return to the default settings.

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.

Command Default Level

Level: 12.

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)#
```

58-18 snmp-server enable traps lldp

This command is used to enable the LLDP and LLDP-MED trap state.

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.

Command Default Level

Level: 12.

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)#
```

58-19 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 the 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.

Command Default Level

Level: 12.

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 for eth2/0/1.

```
Switch# configure terminal
Switch(config)# interface eth2/0/1
Switch(config-if)# lldp med notification enable
Switch(config-if)#
```

58-20 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.

Command Default Level

Level: 12.

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 ethernet 1/0/1
Switch(config-if)# lldp subtype port-id mac-address
Switch(config-if)#
```

58-21 show lldp

This command is used to display the switch’s general LLDP configuration.

show lldp

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the LLDP system's global configurations.

Example

This example shows how to display the LLDP system's global configuration status.

```
Switch# show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-01-02-03-04-00
    System Name               : Switch
    System Description        : TenGigabit Ethernet Switch
    System Capabilities Supported: Repeater, Bridge
    System Capabilities Enabled  : Repeater, Bridge
LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : B1
    Firmware Revision         : 1.10.008
    Software Revision         : 2.00.012
    Serial Number             : D1234567890
    Manufacturer Name         : D-Link
    Model Name                : DXS-3600-16S TenGigabit Ethernet
    Asset ID                  :

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
    Message TX Interval       : 30
    Message TX Hold Multiplier: 4
    ReInit Delay              : 2
    TX Delay                  : 2

LLDP-MED Configuration:
    Fast Start Repeat Count   : 4

Switch#
```

58-22 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 to display the LLDP configuration for a specific interface. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of physical interfaces. No spaces before and after the comma.
-	(Optional) Specifies a range of physical interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the LLDP information of each physical interface.

Example

This example shows how to display a specific physical interface's LLDP configuration.

```
Switch#show lldp interface ethernet 1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID                                                 :eth1/0/1
Admin Status                                            :TX and RX
Notification                                            :Disabled
Basic Management TLVs:
    Port Description                                    :Enabled
    System Name                                         :Enabled
    System Description                                  :Enabled
    System Capabilities                                 :Enabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                        :Enabled
    Enabled Port_and_Protocol_VLAN_ID
        1, 2, 3
    Enabled VLAN Name
        1-3
    Enabled Protocol_Identity
        EAPOL, LACP, GVRP, STP
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                        :Enabled
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled
```

```
LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                                :Enabled
    LLDP-MED Network Policy TLV                              :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV                  :Disabled
    LLDP-MED Inventory TLV                                   :Disabled

LLDP-DCBX Organizationally Specific TLVs:

    LLDP-DCBX ETS Configuration TLV                          :Disabled
    LLDP-DCBX ETS Recommendation TLV                         :Disabled
    LLDP-DCBX Priority-based Flow Control Configuration 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)".

58-23 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 interface's ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays 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 ethernet 1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                             : MAC Address
Port ID                                     : 00-01-02-03-05-00
Port Description                            : D-Link DXS-3600-16S 2.00.012
                                              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                                 : 1.3.6.1.4.1.171.10.118.2

    Address 2 :
        Subtype                             : IPv4
        Address                             : 10.90.90.90
        IF Type                             : IfIndex
        OID                                 : 1.3.6.1.4.1.171.10.118.2

PPVID Entries Count                         : 0
    (None)
VLAN Name Entries Count                     : 1
    Entry 1 :
        VLAN ID                             : 1
        VLAN Name                           : default

Protocol Identity Entries Count             : 0
    (None)
MAC/PHY Configuration/Status                :
    Auto-Negotiation Support                : Supported
    Auto-Negotiation Enabled                : Enabled
    Auto-Negotiation Advertised Capability  : 8000(hex)
    Auto-Negotiation Operational MAU Type   : 0000(hex)
```

```
Link Aggregation                          :
    Aggregation Capability                : Aggregated
    Aggregation Status                    : Not Currently in Aggregation
    Aggregation Port ID                   : 0

Maximum Frame Size                        : 1536

LLDP-MED Capabilities Support:
    Capabilities              :Support
    Network Policy            :Not Support
    Location Identification   :Not Support
    Extended Power Via MDI PSE :Not Support
    Extended Power Via MDI PD  :Not Support
    Inventory                 :Support

ETS Basic Configuration
   Credit Based Shaper Support : Disabled
   Traffic Classes Supported : 8
   Willing : Disabled

ETS Configuration Priority Assignment
   priority0 : 2
   priority1 : 0
   priority2 : 1
   priority3 : 3
   priority4 : 4
   priority5 : 5
   priority6 : 6
   priority7 : 7

ETS Configuration Traffic Class Bandwidth
   TC0 : 4
   TC1 : 7
   TC2 : 11
   TC3 : 14
   TC4 : 18
   TC5 : 21
   TC6 : 25
   TC7 : 0

ETS Configuration Traffic Selection Algorithm
   TC0 : tsaEnhancedTransmission
   TC1 : tsaEnhancedTransmission
   TC2 : tsaEnhancedTransmission
   TC3 : tsaEnhancedTransmission
   TC4 : tsaEnhancedTransmission
   TC5 : tsaEnhancedTransmission
   TC6 : tsaEnhancedTransmission
   TC7 : tsaStrictPriority

ETS Recommendation Traffic Class Bandwidth
   TC0 : 4
   TC1 : 7
```

```
   TC2 : 11
   TC3 : 14
   TC4 : 18
   TC5 : 21
   TC6 : 25
   TC7 : 0

ETS Recommendation Traffic Selection Algorithm
   TC0 : tsaEnhancedTransmission
   TC1 : tsaEnhancedTransmission
   TC2 : tsaEnhancedTransmission
   TC3 : tsaEnhancedTransmission
   TC4 : tsaEnhancedTransmission
   TC5 : tsaEnhancedTransmission
   TC6 : tsaEnhancedTransmission
   TC7 : tsaStrictPriority

PFC Basic Configuration
   Willing : Disabled
   MBC : Disabled
   PFC capability : 8

PFC Enable
   priority0 : Disabled
   priority1 : Disabled
   priority2 : Disabled
   priority3 : Disabled
   priority4 : Disabled
   priority5 : Disabled
   priority6 : Disabled
   priority7 : Disabled

Switch#
```

This example shows how to display the local information of port 1 in normal mode.

```
Switch# show lldp local interface ethernet 1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : MAC Address
Port ID                                  : 00-01-02-03-05-00
Port Description                         : D-Link DXS-3600-16S 2.00.012
                                           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
Energy Efficient Ethernet                : (See Detail)
LLDP-MED capabilities                    : (See Detail)
```

```
LLDP-DCBX capabilities                    : (See Detail)

Switch#
```

This example shows how to display local information of port 1 in brief mode.

```
Switch# show lldp local interface ethernet 1 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                           : MAC Address
Port ID                                   : 00-01-02-03-05-00
Port Description                          : D-Link DXS-3600-16S 2.00.012
                                            Port 1 on Unit 1

Switch#
```

58-24 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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                                 : 1.3.6.1.4.1.171.10.118.2
    Advertising Ports                   : -

Address 2 :
-----------------------------------------------
    Subtype                             : IPv4
    Address                             : 10.90.90.90
    IF Type                             : IfIndex
    OID                                 : 1.3.6.1.4.1.171.10.118.2
    Advertising Ports                   : -

Total Entries : 2

Switch#
```

58-25 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 interface ID.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and 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 normal mode.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command display the information learned from the neighbor devices.

Example

This example shows how to display information about neighboring devices learned by LLDP on eth4/0/9 in detailed mode.

```
Switch# show lldp neighbor interface eth4/0/9 detail
```

```
Port ID : eth4/0/9
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 00-01-02-03-04-05
    Port ID Subtype                             : Local
    Port ID                                     : eth1/0/5
    Port Description                            : RMON Port
    System Name                                 : Switch1
    System Description                          : Stackable Ethernet Switch
    System Capabilities Supported               : Repeater, Bridge
    System Capabilities Enabled                 : Repeater, Bridge
    Management Address Count                    : 0
        (None)
    Port VLAN ID                                : 0
    PPVID Entries Count                         : 0
        (None)
    VLAN Name Entries Count                     : 0
        (None)
    Protocol ID Entries Count                   : 0
        (None)
    MAC/PHY Configuration/Status                : (None)
    Power Via MDI                               : (None)
    Link Aggregation                            : (None)
    Maximum Frame Size                          : 0
    Unknown TLVs Count                          : 0
        (None)
LLDP-MED capabilities                       :
LLDP-MED device class                   : Endpoint device class III
    LLDP-MED capabilities support           :
          LLDP-MED capabilities                 : Support
          Network Policy                        : Support
          Location identification               : Not Support
          Extended power via MDI                : Support
          Inventory                             : Support
       LLDP-MED capabilities enabled              :
          LLDP-MED capabilities                   : Enabled
          Network Policy                          : Enabled
          Location identification                 : Enabled
          Extended power via MDI                  : Enabled
          Inventory                               : Enabled
   Extended power via MDI                         :
             Power device type                    : PD device
             Power Source                         : from PSE
             Power request                        : 8 watts
Network policy                              :
        Application type                        : Voice
        VLAN ID                                 : -
        Priority                                : -
        DSCP                                    : -
        Unknown                                 : True
        Tagged                                  : -
```

```
    Inventory Management                    :
        (None)

Switch#
```

This example shows how to display remote LLDP information in the normal mode.

```
Switch# show lldp neighbor interface eth3/0/1

Port ID : 1
------------------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype           : MAC Address
      Chassis ID                   : 00-01-02-03-04-01
      Port ID Subtype              : Local
      Port ID                      : eth3/0/1
      Port Description             : RMON Port 3 on Unit 1
      System Name                  : Switch1
      System Description           : Stackable Ethernet Switch
      System Capabilities Supported : Repeater, Bridge
      System Capabilities Enabled : Repeater, Bridge
      Management Address Count     : 1
      Port VLAN ID                 : 1
      PPVID Entries Count          : 5
      VLAN Name Entries Count      : 3
      Protocol ID Entries Count    : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                : (See Detail)
      Link Aggregation             : (See Detail)
      Maximum Frame Size           : 1536
LLDP-MED capabilities              : (See Detail)
      Network policy               : (See Detail)
Extended Power Via MDI             : (See Detail)
    Inventory Management           : (See Detail)
    Unknown TLVs Count             : 2
Entity 2
      Chassis ID Subtype           : MAC Address
      Chassis ID                   : 00-01-02-03-04-02
      Port ID Subtype              : Local
      Port ID                      : eth2/0/1
      Port Description             : RMON Port 1 on Unit 2
      System Name                  : Switch2
      System Description           : Stackable Ethernet Switch
System Capabilities Supported : Repeater, Bridge
System Capabilities Enabled   : Repeater, Bridge
      Management Address Count     : 2
      Port VLAN ID                 : 1
      PPVID Entries Count          : 5
      VLAN Name Entries Count      : 3
      Protocol Id Entries Count    : 2
      MAC/PHY Configuration Status  : (See Detail)
      Power Via MDI                : (See Detail)
      Link Aggregation             : (See Detail)
```

```
      Maximum Frame Size            : 1536
      LLDP-MED capabilities         : (See Detail)
      Extended power via MDI        : (See Detail)
Network policy                      : (See Detail)
    Inventory Management            : (See Detail)
Unknown TLVs Count            : 2

Switch#
```

This example shows how to display the neighbor information on eth3/0/1 to eth3/0/2 in brief mode.

```
Switch# show lldp neighbor interface eth3/0/1-3/0/2 brief

Port ID: eth3/0/1
------------------------------------------------------------
Remote Entities Count : 2
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-01
      Port ID Subtype               : Local
      Port ID                       : eth3/0/1
      Port Description              : RMON Port 1 on Unit 3
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-02
      Port ID Subtype               : Local
      Port ID                       : eth4/0/1
      Port Description              : RMON Port 1 on Unit 4

Port ID : eth3/0/2
------------------------------------------------------------------------
Remote Entities Count : 3
Entity 1
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-03
      Port ID Subtype               : Local
      Port ID                       : eth2/0/1
      Port Description              : RMON Port 2 on Unit 1
Entity 2
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-04
      Port ID Subtype               : Local
      Port ID                       : eth2/0/2
      Port Description              : RMON Port 2 on Unit 2
Entity 3
      Chassis ID Subtype            : MAC Address
      Chassis ID                    : 00-01-02-03-04-05
      Port ID Subtype               : Local
      Port ID                       : eth3/0/2
      Port Description              : RMON Port 2 on Unit 3

Total Entries: 2

Switch#
```

58-26 show lldp traffic

This command is used to display the system's global LLDP traffic information.

show lldp traffic

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The global LLDP traffic information displays 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   : 7958183
Total Inserts      : 7
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.

58-27 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 interface ID.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays LLDP traffic on each physical interface.

Example

This example shows how to display statistics information of port 1.

```
Switch#show lldp traffic interface ethernet 1/0/1

Port ID : eth1/0/1
-------------------------------------------
    Total Transmits     : 0
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 0
    Total TLV Discards  : 0
    Total TLV Unknows   : 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.

59. Loopback Detection (LBD) Commands

59-1 loopback-detection (Global)

This command is used to enable the loopback detection function globally. Use the **no** form of the 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	Specifies that the loop detection will work in the port-based mode.
vlan-based	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.

Command Default Level

Level: 12.

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)#
```

59-2 loopback-detection (Interface)

This command is used to enable the loopback detection function for an interface. Use **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the loopback detection function on an interface. This command is available for port and port-channel interface configuration.

Example

This example shows how to enable the loopback detection function on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# loopback-detection
Switch(config-if)#
```

59-3 loopback-detection interval

This command is used to configure the timer interval. Use **no** command to return to the default settings.

loopback-detection interval *SECONDS*

no loopback-detection interval

Parameters

interval *SECONDS*	Specifies the interval in seconds at which CPT packets are transmitted. The valid range is from 1 to 32767.

Default

By default, this value is 10 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

59-4 loopback-detection vlan

This command is used to configure the VLANs to be enabled for loop detection. Use **no** command to return to the default settings.

loopback-detection vlan *VLAN-LIST*

no loopback-detection vlan *VLAN-LIST*

Parameters

VLAN-LIST	(Optional) 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.

Command Default Level

Level: 12.

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.

If the VLAN ID list is empty, 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)#
```

59-5 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 interface's ID to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces are allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the loopback detection setting and status.

Example

This example shows how to displays the current loopback detection settings and status.

```
Switch# show loopback-detection

Loop Detection : Enabled
Detection Mode : vlan-based
LBD enabled VLAN : all VLANs
Interval         : 20 seconds

Interface      Result           Time Left(sec)
-------------- ----------------- ------------
```

```
eth3/0/1        Normal                -
eth3/0/8        Normal                -
eth4/0/6        Loop on vlan 2         120
                Loop on vlan 3         115
…
port-channel1   Loop                   50
port-channel2   Normal                -

Switch#
```

This example shows how to displays the loopback detection status for port 1/0/1.

```
Switch# show loopback-detection interface eth1/0/1

Interface        Result           Time Left(sec)
------------ ------------------ ------------
eth1/0/1         Normal              -

Switch#
```

This example shows how to displays the loopback detection status for port-channel 2.

```
Switch# show loopback-detection interface port-channel2

Interface        Result           Time Left(sec)
------------ ------------------ ------------
port-channel2      Normal              -

Switch#
```

Display Parameters

Interface	Indicates the port that has loopback detection enabled.
Result	Indicates whether a loop is detected.
Time Left	The remaining time before being auto-recovered.

60. MAC Authentication Commands

60-1 mac-auth system-auth-control

This command is used to enable MAC authentication globally. Use the **no** form of the command to disable the MAC authentication globally.

mac-auth system-auth-control

no mac-auth system-auth-control

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

MAC authentication is a feature designed to authenticate a user by MAC address when the user is trying to access the network via the switch. The switch itself can perform the authentication based on a local database or be a RADIUS client and perform the authentication process via the RADIUS protocol with a remote RADIUS server.

Example

This example shows how to enable MAC authentication globally.

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

60-2 mac-auth enable

This command is used to enable MAC authentication on the specified interface. Use the **no** form of the command to disable MAC authentication.

mac-auth enable

no mac-auth enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration. It can be used to enable MAC authentication on the specified interface.

In addition, MAC authentication has the following limitations:

- The MAC authentication port cannot be enabled when port security is enabled on the port.
- The MAC authentication port cannot be enabled when IP-MAC-Port-Binding is enabled on the port.
- The MAC authentication port cannot be enabled on a link aggregation port.

Example

This example shows how to enable MAC authentication on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mac-auth enable
Switch(config-if)#
```

60-3 mac-auth password

This command is used to configure the password of authentication for local and RADIUS authentication. Use the **no** form of this command to reset the password to the default setting.

mac-auth password [0 | 7] *STRING*

no mac-auth password

Parameters

0	(Optional) Specifies the password in the clear text form. If neither 0 nor 7 are specified, the default form will be clear text.
7	(Optional) Specifies the password in the encrypted form. If neither 0 nor 7 are specified, the default form will be clear text.
password *STRING*	Specifies to set the password for MAC authentication. If in the clear text form, the length of the string cannot be over 16 characters.

Default

By default, the password is the client's MAC address.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the password used in the authentication of MAC address users. If the command is not configured, the password for authentication of the MAC address user is formatted based

on the MAC address. The MAC addresses format can be configured with the **authentication mac username format** command.

Example

This example shows how to configure the password for MAC authentication.

```
Switch# configure terminal
Switch(config)# mac-auth password newpass
Switch(config)#
```

60-4 mac-auth username

This command is used to configure the username of local and RADIUS authentication. Use the **no** form of this command to restore the username to the client's MAC address.

mac-auth username *STRING*

no mac-auth username

Parameters

username *STRING*	Specifies the username for MAC authentication. The length of the string cannot be over 16 characters.

Default

By default, the username is the client's MAC address.

Command Mode

Global Configuration Mode,

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the username used in the authentication of MAC address users. The username is used in the authentication via both the local database and remote servers. If the command is not configured, the username for authentication of the MAC address user is formatted based on the MAC address.

Example

This example shows how to configure the username for MAC authentication.

```
Switch# configure terminal
Switch(config)# mac-auth username alpha
Switch(config)#
```

61. Mirror Commands

61-1 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 the 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 valid range is 1 to 4.
interface *INTERFACE-ID*	Specifies the destination interface for the port monitor session.

Default

A session is a local monitor session without destination interfaces.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the destination interface for a local monitor session or the destination interface on the destination switch for an RSPAN 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.

This command is used to configure the destination switch of an RSPAN session. Also, use the **monitor session source remote vlan** command to configure the VLAN that the monitored source packets are tunneled to the switch from the remote site.

Example

This example shows how to create a port monitor session with the session number 1. It assigns a physical port ethernet1/0/1 as the destination port and three physical source ports (ethernet1/0/2 to ethernet1/0/4) as monitor source ports.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface ethernet1/0/1
Switch(config)# monitor session 1 source interface ethernet1/0/2-4
Switch(config)#
```

61-2 monitor session destination remote vlan

This command is used to configure the RSPAN VLAN and destination port for an RSPAN source session. Use the **no** form of the command to remove the configuration of the RSPAN VLAN.

monitor session *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface** *INTERFACE-ID*

no monitor session *SESSION-NUMBER* **destination remote vlan**

Parameters

session *SESSION-NUMBER*	Specifies the session number for the port monitor session. The valid range is 1 to 4.
remote vlan *VLAN-ID*	Specifies the RSPAN VLAN used to tunnel the monitored packets to the remote site. The valid range is 2 to 4094.
interface *INTERFACE-ID*	Specifies the interface to transmit the monitored packets to the remote site.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command on the source switch of an RSPAN session.

The **monitor session destination remote vlan** command configures the destination port used to transmit the monitor packets and the RSPAN VLAN used to tag the monitored packets to the remote site. For each session, only one destination interface can be configured. The destination port does not need to be the member port of the RSPAN VLAN. The destination port can be either a physical port or a port channel.

Each session should be configured with a unique RSPAN VLAN. The user cannot specify an interface for the command to transmit the monitored packets for multiple RSPAN sessions.

Use the **monitor session source interface** command to configure the source ports whose packets will be monitored.

Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN. The monitored packet will be tunneled over the trunk member port of the RSPAN VLAN in the subsequent switches.

Example

This example shows how to create an RSPAN session on the source switch. It assigns VLAN 100 as the RSPAN VLAN with the destination interface ethernet1/0/6 and three source ports (ethernet1/0/2 to ethernet1/0/4) as the port being monitored.

```
Switch# configure terminal
Switch(config)# monitor session 2 source interface ethernet1/0/2-4
Switch(config)# monitor session 2 destination remote vlan 100 interface ethernet1/0/6
Switch(config)#
```

61-3 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* **[, | -]**

Parameters

session *SESSION-NUMBER*	Specifies the session number for the port monitor session. The valid range is 1 to 4.
interface *INTERFACE-ID*	Specifies the source interface for a port monitor session.
,	(Optional) Specifies the number of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and 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.

Default

No monitor function is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 transmitted and received traffic are monitored.

Example

This example shows how to create a port monitor session with session number 1. It assigns a physical port ethernet1/0/1 as a destination port and three source physical ports (ethernet1/0/2 to ethernet1/0/4) as monitor source ports.

```
Switch# configure terminal
Switch(config)# monitor session 1 destination interface ethernet1/0/1
Switch(config)# monitor session 1 source interface ethernet1/0/2-4
Switch(config)#
```

61-4 monitor session source acl

This command is used to configure an access list for flow-based monitoring. Use the **no** form of this command to remove an access list for flow-based monitoring.

monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

no monitor session *SESSION-NUMBER* **source acl** *ACCESS-LIST-NAME*

Parameters

session *SESSION-NUMBER*	Specifies the session number for the port monitor session. The valid range is 1 to 4.
acl *ACCESS-LIST-NAME*	Specifies the flow-based mirror.

Default

No monitor function is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Multiple access lists can be monitored on a session at a time.

Example

This example shows how to create a monitor session with the session number 2. It assigns the MAC access list MAC-Monitored-flow as the monitor source.

```
Switch# configure terminal
Switch(config)# monitor session 2 destination interface ethernet1/0/1
Switch(config)# monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

61-5 monitor session source remote vlan

This command is used to configure the RSPAN VLAN for an RSPAN destination session. Use the **no** form of the command to remove configuration of the RSPAN VLAN.

monitor session *SESSION-NUMBER* **source remote vlan** *VLAN-ID*

no monitor session *SESSION-NUMBER* **source remote vlan**

Parameters

session *SESSION-NUMBER*	Specifies the session number of the port mirroring session. The valid range is 1 to 4.
vlan *VLAN-ID*	Specifies the VLAN that the monitored source packets are tunneled over from the remote site. The valid range is 2 to 4094.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command on the destination switch of an RSPAN session.

The **monitor session source remote vlan** command configures the VLAN that the monitored source packets are tunneled to the switch from the remote site. Use the **monitor session destination interface** command to configure the destination port to transmit the monitored packet.

Each session should be configured with a unique RSPAN VLAN. Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN.

Example

This example shows how to create an RSPAN session on the destination switch. It assigns VLAN 100 as the RSPAN VLAN and ethernet1/0/4 as the destination port. It also assigns VLAN 100 as the RSPAN VLAN. The monitored packets arrive at port ethernet2/0/1 and will be transmitted out from port ethernet1/0/4.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)# exit
Switch(config)# interface ethernet2/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet1/0/4
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 100
Switch(config-if)# exit
Switch(config)# monitor session 2 source remote vlan 100
Switch(config)# monitor session 2 destination interface ethernet1/0/4
Switch(config)#
```

61-6 remote-span

This command is used to specify a VLAN as an RSPAN VLAN. Use the **no** form of the command to revert to a non-RSPAN VLAN.

remote-span

no remote-span

Parameters

None.

Default

None.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **remote-span** command in the VLAN configuration mode to specify a VLAN as an RSPAN VLAN. When a VLAN is specified as an RSPAN VLAN, the MAC address learning option on the RSPAN VLAN is disabled. Use this command on the middle switch and the destination switch involved in the RSPAN session.

For the middle switch involved in a RSPAN session, the port that the monitored packet arrives and the port that the monitored packets will be transmitted need to be configured as tagged member ports of the RSPAN VLAN.

Example

This example shows how to assign VLAN 100 as the RSPAN VLAN in the middle switch of the RSPAN session. Interface ethernet3/0/1 is where the monitored packets arrive and ethernet3/0/5 is where the monitored packet is transmitted.

```
Switch# configure terminal
Switch(config)# interface ethernet3/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# interface ethernet3/0/5
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport trunk allowed vlan 100
Switch(config-if)# exit
Switch(config)# vlan 100
Switch(config-vlan)# remote-span
Switch(config-vlan)#
```

61-7 show monitor session

This command is used to display all or a specific port mirroring session.

show monitor session [*SESSION-NUMBER* **| remote | local]**

Parameters

SESSION-NUMBER	(Optional) Specifies the session number which you want to display.
local	(Optional) Specifies to display the local session.
remote	(Optional) Specifies to display the remote RSPAN session.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If this command is used without specifying a session number, all monitor sessions are 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: Ethernet1/0/1
   Source Ports:
      Both:
          Ethernet1/0/2
          Ethernet1/0/3
          Ethernet1/0/4
      RX:
          Ethernet1/0/5
      TX:
          Ethernet1/0/7

Total Entries: 1

Switch#
```

62. MLD Proxy Commands

62-1 ipv6 mld proxy

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

ipv6 mld proxy

no ipv6 mld proxy

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The MLD proxy only works in a simple tree topology. Make sure there are no other multicast routers except for the proxy devices in the simple tree topology.

When receiving MLD report packet from a downstream interface, MLD proxy will update its membership database which is generated by the merger of all subscriptions on any downstream interface. If the database is changed, the proxy device will send unsolicited reports or leaves from upstream interface. It can also send membership reports from the upstream interface when queried.

Example

This example shows how to enable the MLD proxy on the device.

```
Switch# configure terminal
Switch(config)# ipv6 mld proxy
Switch(config)#
```

62-2 ipv6 mld proxy upstream

This command is used to allow users to configure an interface as the upstream in MLD proxy. Use the **no** form of this command to disable the proxy function on the interface.

ipv6 mld proxy upstream

no ipv6 mld proxy upstream

Parameters

None.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface has an IPv6 address configured. Only one upstream can exist in an MLD proxy device. Upstream performs the host portion of the MLD (RFC2710, RFC3810).

Example

This example shows how to configure the interface VLAN 3 to act as the proxy upstream interface.

```
Switch# configure terminal
Switch(config)# interface vlan3
Switch(config-if)# ipv6 mld proxy upstream
Switch(config-if)#
```

62-3 ipv6 mld proxy downstream

This command is used to configure an interface as a downstream in MLD proxy. Use the **no** form of this command to disable the proxy function on the interface.

ipv6 mld proxy downstream

no ipv6 mld proxy downstream

Parameters

None.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface has IP address configured. Multiple downstream interfaces can be configured on an MLD proxy device. It performs the router portion of the MLD protocol on each downstream interface.

Example

This example shows how to configure the interface VLAN 4 to act as the proxy downstream interface.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if)# ipv6 mld proxy downstream
Switch(config-if)#
```

62-4 ipv6 mld proxy designated-forwarding

This command is used to enable designated forwarding on a non-querier MLD proxy downstream interface. Use the **no** form of this command to disable it.

ipv6 mld proxy designated-forwarding

no ipv6 mld proxy designated-forwarding

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface has an IP address configured.

To avoid local loops and redundant traffic for links that are considered downstream links by multiple MLD-based forwarders, MLD proxy uses the MLD querier election to elect a single forwarder on a LAN. Administrators can use this command to make a non-querier device to be forwarder. Use the configuration in the appropriate topology. Improper usage may cause local loops or redundant traffic.

This command does not take effect if the interface is not set as the downstream interface or set as upstream interface.

Example

This example shows how to enable designated forwarding on downstream interface VLAN 4.

```
Switch# configure terminal
Switch(config)# interface vlan4
Switch(config-if)# ipv6 mld proxy designated-forwarding
Switch(config-if)#
```

62-5 show ipv6 mld proxy

This command is used to display MLD proxy configurations.

show ipv6 mld proxy

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the upstream interface configurations and downstream interfaces.

Example

This example shows how to display the MLD proxy configurations on the device.

```
Switch# show ipv6 mld proxy

MLD Proxy Global State:    Enabled
Upstream Interface:        vlan14
Downstream Interface:
vlan11, vlan12(DF), vlan13(DF)

Switch#
```

62-6 show ipv6 mld proxy group

This command is used to display multicast groups learned by the MLD proxy function.

show ipv6 mld proxy group [*GROUP-ADDRESS***]**

Parameters

GROUP-ADDRESS	Specifies the IPv6 multicast address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all group information by not specifying group address.

Example

This example shows how to display the groups learned by the MLD proxy function.

```
Switch# show ipv6 mld proxy group

FF1E::330E:32, Exclude
Source list: 2000::2, 2000::3

FF1E::EC20:1, Include
Source list: 100::1
```

```
Total entries: 2

Switch#
```

This example shows how to display detailed information of group FF1E::330E:32.

```
Switch# show ipv6 mld proxy group FF1E::330E:32

FF1E::330E:32, Include
Source list: 100::1

Total Entries: 1

Switch#
```

62-7 show ipv6 mld proxy forwarding

This command is used to display multicast forwarding entries created by the MLD proxy function.

show ipv6 mld proxy forwarding [*GROUP-ADDRESS***]**

Parameters

GROUP-ADDRESS	Specifies the IPv6 multicast address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all MLD proxy forwarding information by not specifying the group address.

Example

This example shows how to display the forwarding information created by the MLD proxy function.

```
Switch# show ipv6 mld proxy forwarding

FF1E::330E:32, 2000::2, vlan52
outgoing interface:
vlan20, vlan30

FF1E::EC20:1, 100::1, vlan52
outgoing interface:
vlan20

Total Entries: 2
```

```
Switch#
```

This example shows how to display detailed information of the group FF1E::330E:32.

```
Switch# show ipv6 mld proxy forwarding FF1E::330E:32

FF1E::330E:32, 2000::2, vlan52
outgoing interface:
vlan20, vlan30

Total Entries: 1

Switch#
```

63. MLD Snooping Commands

63-1 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 used. If no VLAN is specified, statistics for all VLANs are cleared.
interface *INTERFACE-ID*	Specifies the interface used.

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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#
```

63-2 ipv6 mld snooping

This command is used to enable or disable MLD snooping.

ipv6 mld snooping

no ipv6 mld snooping

Parameters

None.

Default

MLD snooping is disabled on all VLAN interfaces.

The MLD snooping global state is disabled by default.

Command Mode

Interface Configuration Mode.

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

For a VLAN to operate with MLD snooping, both the global state and per interface 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 operation on all VLANs.

```
Switch# configure terminal
Switch(config)# no ipv6 mld snooping
Switch(config)#
```

This example shows how to enable MLD snooping operation on VLANs that are MLD snooping enabled.

```
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)#
```

63-3 ipv6 mld snooping fast-leave

This command is used to configure MLD snooping fast-leave on the interface. Use the **no** form of the command to disable the fast-leave or option on the specified interface.

ipv6 mld snooping fast-leave

no ipv6 mld snooping fast-leave

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. The **ipv6 mld snooping fast-leave** command allows MLD membership to be removed from a port right on 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)#
```

63-4 ipv6 mld snooping ignore-topology-change-notification

This command is used to make MLD snooping to ignore STP changes and won't send an STP triggered query on the interface. Use the **no** command to make MLD snooping not to ignore STP changes and send an STP triggered query on the specified interface.

ipv6 mld snooping ignore-topology-change-notification

no ipv6 mld snooping ignore-topology-change-notification

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. An MLD snooping switch is aware of link-layer topology changes caused by Spanning Tree operation. When a port is enabled or disabled by the Spanning Tree, a General Query will be sent on all active non-router ports in order to reduce network convergence time. Use this command to make MLD snooping to ignore the topology change case.

Example

This example shows how to enable MLD snooping to ignore topology changes on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping ignore-topology-change-notification
Switch(config-vlan)#
```

63-5 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 the command to revert to 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. On receiving an MLD done message, the MLD snooping querier will assume that there are no local members on the interface 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.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping last-listener-query-interval 3
Switch(config-vlan)#
```

63-6 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 on the VLAN interface 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 an interface or an interface list. No space is allowed before and after the comma. The interface can be a physical interface or a port-channel.
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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. 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 member port of a port channel cannot be specified.

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 eth2/0/1 as an MLD snooping multicast router port and eth1.2 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 eth2/0/1
Switch(config-vlan)# ipv6 mld snooping mrouter forbidden interface eth1/0/2
Switch(config-vlan)#
```

This example shows how to disables the auto-learning of routing protocol packets.

```
Switch# configure terminal
Switch(config)# vlan 4
Switch(config-vlan)# no ipv6 mld snooping mrouter learn pimv6
Switch(config-vlan)#
```

63-7 ipv6 mld snooping proxy-reporting

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

ipv6 mld snooping proxy-reporting [source *IPV6-ADDRESS***]**

no ipv6 mld snooping proxy-reporting

Parameters

IPV6-ADDRESS	(Optional) Specifies the source IP address of proxy reporting.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. The proxy reporting function only works for MLDv1 traffic.

When the function proxy reporting is enabled, the received multiple MLD report or leave packets will be integrated into one report before being sent to the router port. Proxy reporting source IP will be used as source IP of the report, Zero IP address will be used when the proxy reporting source IP is not set. Interface MAC will be used as source MAC of the report. If the VLAN has no IP address configured, then system MAC will be used.

Example

This example shows how to enable MLD snooping proxy-reporting on VLAN 1.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping proxy-reporting
Switch(config-vlan)#
```

63-8 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. The interface must have IPv6 address assigned to start the querier. The system will return warning message if the VLAN has no IPv6 address. If querier is enabled, but IPv6 address is removed, the querier will be stopped.

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. If MLD protocol is also enabled on the interface, MLD Snooping querier state will be disabled automatically.

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)#
```

63-9 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 the 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

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. 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)#
```

63-10 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.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. This command configures 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 an interface.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

63-11 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 {1 | 2}

no ipv6 mld snooping query-version

Parameters

1	Specifies that the version of the MLD general query, sent by MLD snooping querier, is 1.
2	Specifies that the version of the MLD general query, sent by MLD snooping querier, is 2.

Default

By default, this version number is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration.

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)#
```

63-12 ipv6 mld snooping rate-limit

This command is used to configure the upper limit per second for ingress MLD control packets. Use the **no** form of this command to disable the rate limit.

ipv6 mld snooping rate-limit *NUMBER*

no ipv6 mld snooping rate-limit

Parameters

NUMBER	Specifies to configure the rate of the MLD control packet that the switch can process on a specific interface. The rate is specified in packets per second.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is available for VLAN interface configuration, physical port or port-channel interface. The command configures the rate of MLD control packet that is allowed per interface.

Example

This example shows how to limit 30 packets per second on interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping rate-limit 30
Switch(config-vlan)#
```

63-13 ipv6 mld snooping report-suppression

This command is used to enable MLD report suppression on a VLAN. To disable report suppression on a VLAN, use the **no** form of this command.

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. The report suppression function only works for MLDv1 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 MLD report suppression.

```
Switch# configure terminal
Switch(config)# vlan 100
Switch(config-vlan)# ipv6 mld snooping report-suppression
Switch(config-vlan)#
```

63-14 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.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration

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 interface VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# ipv6 mld snooping robustness-variable 3
Switch(config-vlan)#
```

63-15 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 an interface or an interface list. No space is allowed before and after the comma. The interface can be a physical interface or a port-channel.

Default

No static-group is configured.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. This command applies to MLD snooping on a VLAN interface to statically add group membership entries and/or source records.

The **ipv6 mld snooping static-group** command allows the user 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 and/or source records for MLD snooping.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping static-group FF02::12:03 interface eth3/0/5
Switch(config-vlan)#
```

63-16 ipv6 mld snooping suppression-time

This command is used to configure the interval of suppressing duplicate MLD reports or leaves. Use the **no** form of the 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 interval of suppressing duplicates MLD reports. The range is 1 to 300.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. Report suppression function will suppress the duplicate MLD report or leave packets receiving in the suppression time interval. A small suppression time will cause the duplicate MLD packets be sent up 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)#
```

63-17 ipv6 mld snooping minimum-version

This command is used to configure the minimum version of MLD hosts which MLD that is allowed on the interface. Use the **no** form of this command to remove the restriction from the interface.

ipv6 mld snooping minimum-version 2

no ipv6 mld snooping minimum-version

Parameters

None.

Default

No limit on minimum version.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration. This setting only applies to filtering of MLD membership reports.

Example

This example shows how to restrict all MLDv1 hosts to join.

```
Switch# configure terminal
Switch(config)# vlan 1
Switch(config-vlan)# ipv6 mld snooping minimum-version 2
Switch(config-vlan)#
```

63-18 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-ID	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MLD snooping information for all VLANs on which MLD snooping are enabled by not specifying specific VLAN.

Example

This example shows how to display MLD snooping configurations.

```
Switch# show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
  MLD snooping state    : Enabled
  Minimum version       : v2
  Fast leave            : Enabled (host-based)
  Report suppression    : Enabled
  Suppression time      : 10 seconds
  Proxy Reporting       : Disabled
  Mrouter port learning : Enabled
  Querier state         : Enabled (Non-active)
  Query version         : v2
  Query interval        : 125
  Max response time     : 10 seconds
  Robustness value      : 2
  Last listener query interval    : 1 second
  Rate limit            : 50
  Ignore topology change : Disabled

Total Entries: 1

Switch#
```

63-19 show ipv6 mld snooping filter

This command is used to display MLD snooping filter information for all interfaces on the switch or for a specified interface.

show ipv6 mld snooping filter [interface *INTERFACE-ID* **[, | -]]**

Parameters

INTERFACE-ID **[,|-]**	(Optional) Specifies the interface(s) to be displayed. The interface(s) can be a physical interface or a port-channel. If no interface is specified, this command will display MLD snooping filter information on all interface, at which MLD snooping is enabled.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MLD snooping limit and access group information by command.

Example

This example shows how to display filter information when no interface is specified.

```
Switch# show ipv6 mld snooping filter

eth3/0/1:
    Rate limit: 30pps
    Access group: mld_filter
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 25 (Exception List: mld_filter, exceed-action: drop)

eth3/0/3:
    Rate limit: 20pps
    Access group: mld_filter
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: mld_filter
      Groups/Channel Limit: Not Configured
    vlan2:
      Access group: Not Configured
      Groups/Channel Limit: 100 (exceed-action: replace)

port-channel4:
    Rate limit: 200pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured

Switch#
```

63-20 show ipv6 mld snooping groups

This command is used to display MLD snooping group-related information learned on the switch.

show ipv6 mld snooping groups [*IPV6-ADDRESS* **| vlan** *VLAN-ID***]**

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 interface. If no interface is specified, MLD group information about all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MLD group information by command.

Example

This example shows how to display MLD snooping group information.

```
Switch# show ipv6 mld snooping groups

MLD Snooping Connected Group Membership:

VLAN ID  Group address        Source address       FM  Exp(sec)  Interface
-------  -------------------  -------------------  --  --------  ---------
1        FF1E::                        *           EX  258       2/0/7
1        FF1E::3                       *           EX  258       2/0/7
1        FF1E::4               3620:110:1::3a2b    IN  258       2/0/7

Total Entries: 3

Switch#
```

63-21 show ipv6 mld snooping mrouter

This command is used to display MLD snooping multicast router information automatically learned or manually configured on the switch.

show ipv6 mld snooping mrouter [vlan *VLAN-ID* **[,|-]]**

Parameters

vlan *VLAN-ID* **[,|-]**	(Optional) Specifies the VLAN. If no VLAN is specified, MLD snooping Multicast Router Information on all VLANs will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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      eth3/0/4 (static), eth3/0/3 (static)
eth3/0/6 (forbidden)
eth4/0/2 (dynamic)
    2     no mrouter port
3      eth4/0/4 (static)
Eth4/0/3 (dynamic)

Total Entries: 3

Switch#
```

63-22 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 *INTERFACE-ID* **[,|-]**	Specifies the interface of which to display the port statistics counter.
vlan *VLAN-ID* **[,|-]**	Specifies the VLAN of which to display the VLAN statistics.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the MLD snooping related statistics information.

Example

This example shows how to display MLD snooping statistics information.

```
Switch# show ipv6 mld snooping statistics interface

Interface eth4/0/1
Rx: V1Report 1, v2Report 2, Query 1, v1Done 2
Tx: v1Report 1, v2Report 2, Query 1, v1Done 2

Interface eth4/0/3
Rx: V1Report 0, v2Report 0, Query 0, v1Done 0
Tx: v1Report 0, v2Report 0, Query 0, v1Done 0
```

```
Interface eth4/0/4
Rx: V1Report 3, v2Report 0, Query 3, v1Done 0
Tx: v1Report 2, v2Report 2, Query 1, v1Done 2

Total Entries: 3

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#
```

64. Multicast Listener Discovery (MLD) Commands

64-1 ipv6 mld enable

This command is used to enable the MLD protocol state. Use the **no** form of this command to disable the MLD protocol state.

ipv6 mld enable

no ipv6 mld enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. This command only takes effect when the interface has an IPv6 address configured.

Example

This example shows how to enable MLD on VLAN 1.

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

64-2 ipv6 mld last-listener-query-count

This command is used to configure the number of group-specific or group-source specific queries sent before the router assumes there are no local members of a group. Use the **no** form of the command to revert to the default setting.

ipv6 mld last-listener-query-count *VALUE*

no ipv6 mld last-listener-query-count

Parameters

VALUE	Specifies the last member query count. The valid range is 1 to 7.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for VLAN interface configuration. The user can use this command to configure the number of group-specific or group-source specific queries sent before the router assumes there are no local members of a group. If the router does not receive reports from hosts within the timeout period, the router will stop sending the multicast group traffic to the interface.

Example

This example shows how to configure MLD last-listener-query-count to 5 for VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ipv6 mld last-listener-query-count 5
Switch(config-if)#
```

64-3 ipv6 mld last-listener-query-interval

This command is used to configure the MLD last listener query interval on an interface. Use the **no** form of the command to revert to the default setting.

ipv6 mld last-listener-query-interval *SECONDS*

no ipv6 mld last-listener-query-interval

Parameters

SECONDS	Specifies the Interval, in seconds for the amount of time between group-specific or group-source-specific queries. The valid range is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available on the VLAN interface configuration. When an MLD querier receives a packet to leave the specific group or channel, it will send a group specific query or group source specific query. The leave timer starts once the MLD querier receives the packet from an interface. If the interface does not receive the report packet before the leave timer expires, then the interface's membership will be removed from the group or channel that is to be leaved. The value of the leave timer is the value of the last-listener-query-interval * the last-listener-query-count.

Example

This example shows how to configure the interval of the last listener query to 2 seconds on VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ipv6 mld last-listener-query-interval 2
Switch(config-if)#
```

64-4 ipv6 mld query-interval

This command is used to configure the interval at which the router sends MLD Multicast Listener Query messages. Use the **no** form of the command to revert to the default setting.

ipv6 mld query-interval *SECONDS*

no ipv6 mld query-interval

Parameters

query-interval *SECONDS*	Specifies to configure the frequency at which the designated router sends MLD general-query messages. The range is from 1 to 31744.

Default

By default, this value is 125 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only valid for the VLAN interface. The user can use this command to modify the MLD query interval on an interface.

The MLD querier will send the general query at the interval specified by the query interval command. On receiving the general query, the MLD listener needs to respond the report packet to claim that it is interested in the specified multicast group.

Example

This example shows how to configure the MLD query interval for VLAN 1000. It configures the MLD query Interval value to 150 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ipv6 mld query-interval 150
Switch(config-if)#
```

64-5 ipv6 mld query-max-response-time

This command is used to configure the maximum response time advertised in MLD queries. To restore the default value, use the **no** form of this command.

ipv6 mld query-max-response-time *SECONDS*

no ipv6 mld query-max-response-time

Parameters

SECONDS	Specifies to set the maximum response time, in seconds, advertised in MLD queries. The range is from 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The valid interface for this command is VLAN. This command controls the period during which the group member can respond to an MLD query message before the router deletes the membership.

Example

This example shows how to configure the MLD query's maximum response time for VLAN 1000. It configures the MLD query maximum response time value to 10 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ipv6 mld query-max-response-time 10
Switch(config-if)#
```

64-6 ipv6 mld robustness-variable

This command is used to set the robustness variable used in MLD. Use the **no** form of this command to revert to the default value.

ipv6 mld robustness-variable *VALUE*

no ipv6 mld robustness-variable

Parameters

VALUE	Specifies the robustness variable. The valid value range is 2 to 7.

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for the VLAN interface configuration.

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 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 MLD robustness variable to 3 for VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ipv6 mld robustness-variable 3
Switch(config-if)#
```

64-7 ipv6 mld version

This command is used to change the MLD version on the specified interface. Use the **no** form of the command to revert to the default setting.

ipv6 mld version {1 | 2}

no ipv6 mld version

Parameters

1	Specifies to configure the switch to run MLD version 1.
2	Specifies to configure the switch to run MLD version 2.

Default

The default MLD version is 2.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for the VLAN interface configuration. The user can use this command to modify the MLD query version on an interface.

Example

This example shows how to configure the MLD version 1.

```
Switch# configure terminal
Switch(config)# interface vlan1000
Switch(config-if)# ipv6 mld version 1
Switch(config-if)#
```

64-8 show ipv6 mld groups

This command is used to display MLD group information on an interface.

show ipv6 mld groups [*GROUP-ADDRESS* **| interface** *INTERFACE-ID***] [detail]**

Parameters

GROUP-ADDRESS	(optional) Specifies to display the group IPv6 address. If no IPv6 address specified, all MLD group information will be displayed.
interface *INTERFACE-ID*	(optional) Specifies the interface to display. If no interface is specified, MLD group information about all interfaces will be displayed.
detail	(Optional) Specifies to display the detailed group information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display multicast group information for a specific group or for a specific interface.

Example

This example shows how to display MLD group information in interface VLAN 1.

```
Switch#show ipv6 mld groups interface vlan1

Group Address                       Interface  Uptime       Expire
------------------------------------------------------------------
FF02::1:FF00:65                     vlan1      0DT00H05M26S 0DT00H01M12S
FF02::1:FF23:86CC                   vlan1      0DT00H03M26S 0DT00H01M55S
FF02::4:FF00:1                      vlan1      0DT00H04M12S Stopped
Total Entries: 3

Switch#
```

This example shows how to display MLD group detailed information of group ff02::1:ff23:86cc.

```
Switch# show ipv6 mld groups ff02::1:ff23:86cc detail

Interface     : vlan1
Group         : FF02::1:FF23:86CC
```

```
Uptime        : 0DT00H00M42S
Expires       : Stopped
Group mode    : Include
Last reporter : FE80::202:B3FF:FEF0:79D8

Group source list:
       Source Address               Uptime        Expire
       ------------------------------------------------
       2004:4::6                    0DT00H00M42S  0DT00H03M38S
       Total Source Entries: 1
Total Entries: 1

Switch#
```

Display Parameters

Uptime	The time elapsed since the entry has been created in the format of [n]DT[n]H[n]M[n]S.
Expires	The time that the entry will be removed if there is no refresh on the entry in the format of [n]DT[n]H[n]M[n]S. Stopped indicates that the timing out of this entry is not determined by this expire timer. If the router is in Include mode for a group, then the whole group entry times out after the last source entry has timed out (unless the mode is changed to Exclude mode before it times out).
Group mode	Include or Exclude: The group mode is based on the type of membership reports that are received on the interface for the group.
Last reporter	Last host to report being a member of the multicast group.

64-9 show ipv6 mld interface

This command is used to display MLD information on the switch.

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

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, MLD information about all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MLD information on all interfaces.

Example

This example shows how to display MLD interface information on VLAN 1000.

```
Switch# show ipv6 mld interface vlan1000

VLAN 1000
Version                         : 2
IPv6 Address/Netmask            : FE80::260:3EFF:FE86:5649/10
MLD State                       : Enabled
Querier                          : FE80::233:1265:3322:6387
Query Interval                  : 125 seconds
Query Maximum Response Time     : 10 seconds
Robustness Variable             : 3
Last Listener Query Count       : 2
Last Listener Query Interval    : 1 seconds

Switch#
```

Display Parameters

Version	The MLD protocol version running on the interface.
Querier	The querier IP on the interface LAN.

65. Multicast VLAN Commands

65-1 mvlan enable

This command is used to enable multicast VLAN and configure some options for the multicast VLAN feature. Use the **no** form of this command to disable the state or return to the default configuration.

mvlan {ipv4 enable | ipv6 enable}

no mvlan {ipv4 enable | ipv6 enable}

Parameters

ipv4 enable	Specifies to enable the IPv4 IGMP control packet process in multicast VLAN.
ipv6 enable	Specifies to enable the IPv6 MLD control packet process in multicast VLAN.

Default

Multicast VLAN for the IPv4 packet process is disabled.

Multicast VLAN for the IPv6 packet process is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable multicast VLAN and configure some options for the multicast VLAN feature.

Example

This example shows how to enable the multicast VLAN feature for IPv4 multicast packets.

```
Switch# configure terminal
Switch(config)# mvlan ipv4 enable
Switch(config)#
```

65-2 mvlan

This command is used to configure characteristics of the multicast VLAN feature. Use the **no** form of this command to return to the default configuration.

mvlan {forward-unmatched | ignore-vlan}

no mvlan {forward-unmatched | ignore-vlan}

Parameters

forward-unmatched	Specifies that if the received IGMP or MLD control packet is untagged, does not match any profile, and the associated default VLAN is a multicast VLAN, or is tagged with a multicast VLAN, but does not match the associated profile, then the packet will be forwarded or dropped based on this setting. By default, the packet will be dropped.
ignore-vlan	Specifies the setting for tagged IGMP or MLD control packets. If enabled, then the packet's VLAN is ignored and taken to match the profile to find its multicast VLAN. When this option is enabled, the switch will ignore the VLAN of the receiving IGMP or MLD control packet and try to find a match profile.

Default

Forward-unmatched: Disabled.

Ignore VLAN: Disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the untagged IGMP/MLD report/leave/done packets are received by the receiver port, the packets will be matched against the group profile defined for the multicast VLANs that the receiver port belongs to and classified to the matched multicast VLAN. If the packet is matched, then the port will be taken into subsequent group learning process with the matched multicast VLAN.

If there is no match against all multicast VLANs and if the VLAN associated with the packet happens to be a multicast VLAN, the IGMP/MLD packet can be either dropped or flooded to VLAN member ports depending on the setting of this command. If **forward-unmatched** is disabled, then the packet is dropped. If **forward-unmatched** is enabled, then the packet is flooded.

If there are no matches against all multicast VLANs and the packet's VLAN is not configured as the multicast VLAN, then the IGMP/MLD packet will not be handled by multicast VLAN.

If the IGMP/MLD report/leave/done packet received by the receiver port is tagged, then the handling is different based on setting of the **ignore-vlan** parameters.

If packet VLAN is a multicast VLAN and the packet matches the group profile of the VLAN, then the packet will be taken into the subsequent group learning process. If there is no match, then the packet will be handled based on **forward-unmatched** setting. If packet VLAN is not a multicast VLAN, then the packet will not be handled by the multicast VLAN.

If the packet's VLAN is IGMP/MLD snooping enabled, the packet will be processed by IGMP/MLD snooping, or else the packet's VLAN is ignored and taken to match the group profile of multicast VLANs associated with the receive port. If there is a match, then the packet will be taken into the subsequent group learning process with the matched multicast VLAN. If there is no match but the packet's VLAN is a multicast VLAN, then the packet will be handled based on the **forward-unmatched** setting. If the packet VLAN is not a multicast VLAN, then the packet will not be handled by multicast VLAN.

Example

This example shows how to enable the forward unmatched and ignore VLAN setting.

```
Switch# configure terminal
Switch(config)# mvlan forward-unmatched
Switch(config)# mvlan ignore-vlan
Switch(config)#
```

65-3 mvlan vlan

This command is used to create a multicast VLAN. Use the **no** form of this command to remove a multicast VLAN.

mvlan vlan *VLAN-ID*

no mvlan vlan *VLAN-ID*

Parameters

vlan *VLAN-ID*	Specifies the multicast VLAN to create. The range is 1 to 4094.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A VLAN that has been created as an ordinary 802.1Q VLAN cannot be specified as a multicast VLAN and vice versa. A VLAN cannot be IGMP snooping enabled and specified as a multicast VLAN at the same time.

Example

This example shows how to create the multicast VLAN 100.

```
Switch# configure terminal
Switch(config)# mvlan ipv4 enable
Switch(config)# mvlan vlan 100
Switch(config-mvlan)#
```

65-4 member

This command is used to configure interfaces as source ports or as receiver ports of a multicast VLAN. Use the **no** form of this command to remove receiver ports or source ports.

member {receiver | source} {tagged | untagged} *INTERFACE-ID* **[, | -]**

no member {receiver | source} INTERFACE-ID [, | -]

Parameters

receiver	Specifies to configure the port as a subscriber port that can only receive multicast data in the multicast VLAN.
source	Specifies to configure the port as an uplink port that can send multicast data in the multicast VLAN.
Tagged	Specifies that if a port is a tagged member, the packets sent from the port are tagged with the Multicast VLAN ID.

untagged	Specifies that if the port is an untagged member, then the packets will be forwarded in the untagged form.
INTERFACE-ID	Specifies an interface or an interface list. No spaces are allowed before and after the comma. The interface can be a physical interface or a port-channel.

Default

No receiver or source port is a member of any multicast VLAN.

Command Mode

Multicast VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The member port of a multicast VLAN can be either a receiver port or a source port. Receiver ports are ports connected to subscribers. Source ports are ports that the multicast traffic source comes from.

A multicast VLAN can have more than one source ports. If IGMP/MLD report packets come from a source port, Multicast VLAN will not learn the IGMP/MLD group for this report, but only forward the packets to other source ports in the Multicast VLAN.

A port can be the receiver port of multiple multicast VLANs at the same time.

There are some restrictions when configuring receiver and source ports for a Multicast VLAN.

- In a single Multicast VLAN, a port cannot be a receiver port and a source port at the same time.
- The source ports in a single Multicast VLAN must all be either tagged members or untagged members.
- Tagged receiver ports cannot overlap with untagged receiver ports in a single Multicast VLAN.
- Source ports in one Multicast VLAN cannot overlap with receiver ports between two Multicast VLANs.
- Tagged source ports cannot overlap untagged source ports between two Multicast VLANs.

Example

This example shows how to configure ports eth1/0/1 to eth1/0/4 as tagged receiver ports in multicast VLAN 100.

```
Switch# configure terminal
Switch(config)# mvlan
Switch(config)# mvlan 100
Switch(config-mvlan)# member receiver tagged eth1/0/1-4
Switch(config-mvlan)#
```

65-5 name

This command is used to specify the name of a multicast VLAN. Use the **no** form of this command to reset the VLAN name to the default VLAN name.

name *VLAN-NAME*

no name

Parameters

VLAN-NAME	Specifies the VLAN name, with a maximum of 32 characters.

Default

The default multicast VLAN name is MVLANxxxx, where xxxx represents four numeric digits (including the leading zero) that are equal to the VLAN ID.

Command Mode

Multicast VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the name of a multicast VLAN.

Example

This example shows how to configure the multicast VLAN name of multicast VLAN 100 to “ip-tv”.

```
Switch# configure terminal
Switch(config)# mvlan
Switch(config)# mvlan 100
Switch(config-mvlan)# name ip-tv
Switch(config-mvlan)#
```

65-6 replace-priority

This command is used to replace the priority of data traffic forwarded in the multicast VLAN. Use the **no** form of this command to cancel the priority replacement.

replace-priority {ipv4 *PRIORITY* **| ipv6** *PRIORITY***}**

no replace-priority {ipv4 | ipv6}

Parameters

ipv4 *PRIORITY*	Specifies the remap priority for IPv4 multicast packets forwarded on the multicast VLAN.
ipv6 *PRIORITY*	Specifies the remap priority for IPv6 multicast packets forwarded on the multicast VLAN.

Default

None.

Command Mode

Multicast VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the replacing priority option is configured, the multicast data packets forwarded on the multicast VLAN will be tagged with the replacing priority option. Otherwise the priority is the value of the original packet.

Example

This example shows how to configure replacing the IPv4 packet priority to 4.

```
Switch# configure terminal
Switch(config)# mvlan
Switch(config)# mvlan 100
Switch(config-mvlan)# replace-priority ipv4 4
Switch(config-mvlan)#
```

65-7 replace-source-ip

This command is used to configure the source IP address which will be replaced into the reporting IGMP/MLD packet to uplink ports. Use the **no** form of this command to cancel the source address replacing.

replace-source-ip {ipv4 *IPV4-ADDRESS* **| ipv6** *IPV6-ADDRESS***} from {souce | receiver | both}**

no replace-source-ip {ipv4 | ipv6}

Parameters

ipv4 *IPV4-ADDRESS*	Specifies the source IP address for IGMP control packet reporting up to routers.
ipv6 *IPV6-ADDRESS*	Specifies the source IP address for MLD control packet reporting up to routers.
source	Specifies that the source IP address of the IGMP report/leave packet received on any multicast VLAN source port will be replaced.
receiver	Specifies that the source IP address of the IGMP report/leave packet received on any multicast VLAN receiver port will be replaced.
both	Specifies that the source IP address of the IGMP report/leave packet received on any port in the multicast VLAN will be replaced.

Default

None.

Command Mode

Multicast VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The replace source IP option is used while reporting the join information towards the source port. The purpose is to avoid the control packets dropped by the uplink router due to IP spoofing checks.

If the replacing address is configured, before forwarding the IGMP/MLD report/leave/done packet, sent by the host, the source IP address in the report/leave/done packet will be replaced by this IP address. Otherwise, the source IP address will not be replaced.

Example

This example shows how to configure the IPv4 and IPv6 replacing source address.

```
Switch# configure terminal
```

```
Switch(config)# mvlan
Switch(config)# mvlan 100
Switch(config-mvlan)# replace-source-ip ipv4 1.10.10.10 from receiver
Switch(config-mvlan)# replace-source-ip ipv6 FE80:3000::3 from source
Switch(config-mvlan)#
```

65-8 mvlan group-profile

This command is used to create a group profile for the multicast VLAN feature. Use the **no** form of this command to remove a group profile or all group profiles.

mvlan group-profile *PROFILE-NAME*

no mvlan group-profile {*PROFILE-NAME* **| all}**

Parameters

PROFILE-NAME	Specifies the name of the profile.
all	Specifies to remove all multicast VLAN profiles.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A profile is used to define group address ranges. It will be used by multicast VLANs to check which multicast VLAN should be replaced through matching the group in the IGMP/MLD packet.

Example

This example shows how to create a profile named “mv_profile1”.

```
Switch# configure terminal
Switch(config)# mvlan group-profile mv_profile1
Switch(config-mvlan-profile)#
```

65-9 access-group

This command is used to bind an access group profile to a multicast VLAN. Use the **no** form of this command to remove the binding.

access-group *PROFILE-NAME*

no access-group *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the profile.

Default

None.

Command Mode

Multicast VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A single Multicast VLAN can be bound with more than one profile as its real group range. Group ranges cannot overlap among Multicast VLANs. A port can be member port of multiple multicast VLANs. If it is the case, then the group permitted by the access group configured for the Multicast VLAN will be learned with this multicast VLAN.

If a port is member port of a single multicast VLAN, if access group is configured for the multicast VLAN, then only those group permitted by the access group are learned with the multicast VLAN. If there is no access group configured, then all multicast group will be learned with the multicast VLAN.

Example

This example shows how to bind the profile “mv_profile1” to multicast VLAN 100.

```
Switch# configure terminal
Switch(config)# mvlan 100
Switch(config-mvlan)# access-group mv_profile1
Switch(config-mvlan)#
```

65-10 range

This command is used to configure the multicast address range for a multicast VLAN profile. Use the **no** form of this command to remove a range.

range {*IPV4-ADDRESS-START* **[***IPV4-ADDRESS-END***] |** *IPV6-ADDRESS-START* **[***IPV6-ADDRESS-END***]}**

no range {*IPV4-ADDRESS-START* **[***IPV4-ADDRESS-END***] |** *IPV6-ADDRESS-START* **[***IPV6-ADDRESS-END***]}**

Parameters

IPV4-ADDRESS-START	Specifies the IPv4 multicast start address of the range.
IPV4-ADDRESS-END	Specifies the IPv4 multicast end address of the range.
IPV6-ADDRESS-START	Specifies the IPv6 multicast start address of the range.
IPV6-ADDRESS-END	Specifies the IPv6 multicast end address of the range.

Default

None.

Command Mode

Multicast VLAN Profile Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Multiple ranges can be added to a multicast VLAN profile. The IP address ranges, specified in a single profile, must be of the same address family.

Example

This example shows how to add an IPv4 range into the profile called “profile mv_profile1”.

```
Switch# configure terminal
Switch(config)# mvlan group-profile mv_profile1
Switch(config-mvlan-profile)# range 225.0.0.0 225.0.0.5
Switch(config-mvlan-profile)#
```

65-11 show mvlan group-profile

This command is used to display the multicast group profile configuration.

show mvlan group-profile [*PROFILE-NAME***]**

Parameters

PROFILE-NAME	Specifies the profile name.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all group profiles by not specifying the profile name.

Example

This example shows how to display all multicast VLAN profiles.

```
Switch# show mvlan group-profile

Profile Name              Multicast Addresses
--------------------  --------------------------------
mv_profile1               225.0.0.0-225.0.0.5
customer                  224.19.62.34 - 224.19.162.200
IP6-TV1                   FF02::1:ff00:65
IP6-SET                   FF02::4:: - FF02::FF03

Total Entries : 4

Switch#
```

65-12 show mvlan access-group

This command is used to display which multicast group profiles are bound to which multicast VLANs.

show mvlan access-group [*VLAN-ID***]**

Parameters

VLAN-ID	Specifies the VLAN ID.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all binding information by not specifying the VLAN ID.

Example

This example shows how to display the group profiles associated with the multicast VLAN.

```
Switch# show mvlan access-group

Multicast VLAN    Multicast Group Profiles
---------------   --------------------------------
100               mv_profile1, IP6-SET

Total Entries: 1

Switch#
```

65-13 show mvlan

This command is used to display multicast VLAN configurations.

show mvlan [*VLAN-ID***]**

Parameters

VLAN-ID	Specifies the VLAN ID.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all configurations and information of the multicast VLAN by not specifying the VLAN ID.

Example

This example shows how to display all multicast VLAN configurations and information on the switch.

```
Switch# show mvlan

IPv4 Multicast VLAN State    : Enabled
IPv6 Multicast VLAN State    : Disabled
Forward Unmatched: Disabled
Ignore VLAN : Enabled

MVLAN 100
Untagged Receiver        : eth1/0/15
Tagged Receiver          : eth1/0/1-4
Untagged Source          : eth1/0/18
Tagged Source            :
Replace Source IP        : 0.0.0.0 (from source)/FE80::32 (from receiver)
Replace priority               : 4

MVLAN 200
Untagged Receiver        : eth2/0/1-5
Tagged Receiver          :
Untagged Source          :
Tagged Source            : eth1/0/10
Replace Source IP        : 1.0.0.1 (from both)/Not replace
Replace priority               : Not replace

Total Entries: 2

Switch#
```

Display Parameters

IPv4 Multicast VLAN State	The state of the multicast VLAN function to process IPv4 packet. It can be **Disabled** or **Enabled**.
IPv6 Multicast VLAN State	The state of the multicast VLAN function to process IPv6 packets. It can be **Disabled** or **Enabled**.
Forward Unmatched	The forwarding mode for Multicast VLAN unmatched packets. **Enabled** means forward, and **Disabled** means not forward.
Auto Assign VLAN	Automatically assign the IGMP control packets to the right multicast VLAN.
Untagged/Tagged Receiver/Source	The receiver/source ports configured in the multicast VLAN and the VLAN tagged or untagged attribute for multicast packets forwarded towards them.

Replace Source IP	The source IP address that will be replaced in the IGMP/MLD control packets before forwarded in the multicast VLAN.

66. Multiple Spanning Tree Protocol (MSTP) Commands

66-1 instance

This command is used to map a VLAN or a set of VLANs to an MST instance. Use the **no** instance without VLANs specified to remove instances. Use the **no** instance with VLAN specified to return the VLANs to the default instance (CIST).

instance *INSTANCE-ID* **vlans** *VLANDID* **[, | -]**

no instance *INSTANCE-ID* **[vlans** *VLANDID* **[, | -]]**

Parameters

INSTANCE-ID	Specifies the MSTP instance identifier to which the specified VLANs are mapped. This value must be between 1 and 4094.
vlans *VLANDID*	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 VLAN, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLAN. No space is allowed before and after the hyphen.

Default

None.

Command Mode

MST Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Any unmapped VLAN is mapped to the CIST instance. When mapping the VLANs to an instance, if the instance doesn't 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)#
```

66-2 name

This command is used to configure the name of an MST region. To return to the default name, use the **no** form of this command.

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 switch's MAC address.

Command Mode

MST Configuration Mode.

Command Default Level

Level: 12.

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)#
```

66-3 revision

This command is used to configure the revision number for the MST configuration. To return to the default settings, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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)#
```

66-4 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	Specifies to display the table for the mapping relationship between VLANs and MSTP Instances.
digest	Specifies to display the MD5 digest included in the current MST configuration identifier (MSTCI).
instance *INSTANCE-ID* **[, | -]**	Specifies to display the MSTP information for the designated instance only. Define multiple instances by using ‘,’ to specify a series of instances or to separate a range of instances from a previous range. Use ‘-‘ to specify a range of instances. No space before and after the comma or hyphen.
interface *INTERFACE-ID*	Specifies to display the STP information for the specified interface.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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:  enabled,  protocol: MSTP
NNI BPDU Address: Dot1d(01-80-C2-00-00-00)
Number of MST instances: 2

>>>>MST instance: 00,  vlans mapped: 1-2,4-2999,4000-4094
Bridge Address: 00:02.17:2C:F4:00, Priority: 32768 (32768 sysid 0)
Designated Root Address: 00:02.17:2C:F4:00, Priority: 32768
Regional Root Address: 00:02.17:2C.F4:00 , Priority: 32768
Designated Bridge Address: 00:02.17:2C:F4:00, Priority: 32768
Topology Changes Count : 0

eth3/0/1
Port state: forwarding
  Port role: designated
  Port info: port ID 128.1, priority: 128, cost: 20000
  Designated root address: 00:02.17:2C.F4:00, priority: 32768, cost: 0
  Regional root address: 00:02.17:2C.F4:00 , Priority:  32768
  Designated bridge address: 00.02.17.2C.F4.00 priority 32768, port id: 128.1

eth3/0/2
  Port state: forwarding
  Port role: designated
  Port info: port ID: 128.193, priority: 128, cost: 200000
  Designated root address 00:02:17:2C.F4:00, priority: 32768, cost: 0
  Regional root address: 00:02.17:2C.F4:00 , Priority:  32768
  Designated bridge address 00:02:17:2C.F4:00, priority: 32768, port ID: 128.194

eth3/0/3
Port state: blocking
Port role: backup
  Port info: port ID 128.194, priority: 128, cost: 200000
  Designated root address: 00:02:17:2C:F4:00, priority: 32768, cost: 0
  Regional root address: 00:02.17:2C.F4:00 , Priority:  32768
  Designated bridge address: 00:02:17:2C:F4:00, priority 32768, port ID: 128.195

>>>>MST instance: 01,  vlans mapped: 3,3000-3999
Bridge Address: 00:02.17:2C:F4:00, Priority: 32769 (32768 sysid 1)
Designated Root Address: 00:02.17:2C:F4:00, Priority: 32769Designated Bridge Address:
00:02.17:2C:F4:00, Priority: 32769
Topology Changes Count : 0

eth3/0/1
Port state: forwarding
  Port role: designated
  Port info: port ID 128.1, priority: 128, cost: 20000
```

```
  Designated root address: 00:02.17:2C.F4:00, priority: 32771, cost: 0  Designated
bridge address: 00.02.17.2C.F4.00 priority 32771, port id: 128.1

eth3/0/2
  Port state: forwarding
  Port role: designated,
  Port info: port ID: 128.193, priority: 128, cost: 200000
  Designated root address 00:02:17:2C.F4:00, priority: 32771, cost: 0
  Designated bridge address 00:02:17:2C.F4:00, priority: 32771, port ID: 128.193

eth3/0/3
Port state:blocking
Port role: backup,
  Port info: port ID 128.194, priority: 128, cost: 200000
  Designated root address: 00:02:17:2C:F4:00, priority: 32771, cost: 0  Designated
bridge address: 00:02:17:2C:F4:00, priority 32771, port ID: 128.193

Switch#
```

This example shows how to display MSTP detailed information for interface eth3/0/1.

```
Switch# show spanning-tree mst interface eth3/0/1 detail

eth3/0/1
  Configured link type: auto, operation status: point-to-point
  Configured fast-forwarding: auto, operation status: edge
  Bpdu statistic counter: sent: 4, received: 0

  >>>>MST instance: 00,  vlans mapped: 1-2,4-2999,4000-4094  Port state: forwarding
  Port role: designated
  Port info: port ID 128.1, priority: 128, cost: 20000
  Designated root address: 00:02.17:2C.F4:00, priority: 32768, cost: 0
  Regional root address: 00:02.17:2C.F4:00 , Priority: 32768
  Designated bridge address: 00.02.17.2C.F4.00 priority 32768, port id: 128.1

  >>>>MST instance: 01,  vlans mapped: 3,3000-3999
  Port state: forwarding
  Port role: designated
  Port info: port ID 128.1, priority: 128, cost: 20000
  Designated root address: 00:02.17:2C.F4:00, priority: 32771, cost: 0
  Designated bridge address: 00.02.17.2C.F4.00 priority 32771, port id: 128.1

Switch#
```

This example shows how to display MSTP summary information.

```
Switch# show spanning-tree mst

Spanning tree: enabled, protocol: MSTP
NNI BPDU Address: Dot1d(01-80-C2-00-00-00)
Number of MST instances: 2

>>>>>MST00 vlans mapped:   1,4-4094
Bridge Address: 00-12-85-26-05-00,  Priority: 32768 (32768 sysid 1)
```

```
Designated Root Address: 00-54-85-26-05-00, Priority: 4096  (4096 sysid 0)
Regional Root Address: 00-12-85-26-05-00,  Priority: 32768
Designated Bridge Address: 00-12-85-26-05-00,  Priority: 32768
Topology Changes Count : 0

                                          Priority   Link
 Interface  Role       State      Cost    .Port#    Type        Edge
---------  -----      -----      ------  --------- ------      --------
eth3/0/3     designated forwarding 20000     128.3   p2p         edge
eth3/0/5     backup     blocking   200000    128.5   p2p         non-edge
eth3/0/6     backup     blocking   200000    128.6   shared      edge
eth3/0/7     root       forwarding 2000      128.9   p2p         edge

>>>>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
---------  ----       -----      ------  --------- ------      --------
eth3/0/9     designated forwarding 20000     128.9   p2p         edge
eth3/0/10    backup     blocking   200000    128.10  p2p         non-edge
eth3/0/11    cackup     blocking   200000    128.11  shared      edge
eth3/0/12    root       forwarding 2000      128.12  p2p         edge

Switch#
```

This example shows how to display MSTP summary information for interfaces eth3/0/3 to eth 3/0/4.

```
Switch# show spanning-tree mst interface eth3/0/3-4

eth3/0/3
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

eth3/0/4
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 for interfaces eth3/0/3 to eth 3/0/4 of MST02.

```
Switch# show spanning-tree mst instance 2 interface eth3/0/3-4

>>>>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
                                          Priority  Link
   Interface  Role       State      Cost    .Port#    Type        Edge
---------  ----       -----      ------  --------- ------      --------
eth3/0/3    backup     blocking   200000    128.3  p2p         non-edge
eth3/0/4    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     : [region1]
Revision : 2, Instances configured: 3
Instance   Vlans
---------  -------------
0          21-4094
1          1-10
2          11-20

Switch#
```

66-5 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). To return to the default settings, use the **no** form of this command.

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** value depends on the port speed. The faster the interface's speed is will indicate a smaller cost. MST always uses long path costs.

The default **priority** value is 128.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When entering the **cost** value, do not include a comma in the entry. For example, enter 1000, not 1,000.

Example

This example shows how to configure the interface's path cost.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

66-6 spanning-tree mst configuration

This command is used to enter the MST Configuration Mode. To return to the default settings, use the **no** form of this command.

spanning-tree mst configuration

no spanning-tree mst configuration

Parameters

None.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

66-7 spanning-tree mst max-hops

This command is used to configure the MSTP maximum hop count value. Use the **no** form of the command to reset 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.

Command Default Level

Level: 12.

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)#
```

66-8 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 the 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.

Command Default Level

Level: 12.

Usage Guideline

This MSTP hello-time only takes effect in the MSTP mode.

Example

This example shows how to configure the port hello-time to 1 for the Ethernet interface eth1/01.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# spanning-tree mst hello-time 1
Switch(config-if)#
```

66-9 spanning-tree mst priority

This command is used to configure the bridge priority value for the selected MSTP instance. Use the **no** command to return the setting 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.

Command Default Level

Level: 12.

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)#
```

67. Multiprotocol Label Switching (MPLS) Commands

67-1 backoff

This command is used to configure the initial and maximum back-off delay time. Use the **no** form of this command to restore the default value.

backoff *INIT-TIME MAX-TIME*

no backoff

Parameters

INIT-TIME	Specifies the initial back-off delay time. The range is from 15 to 65535 seconds.
MAX-TIME	Specifies the maximum back-off delay time. The range is from 120 to 65535 seconds.

Default

Initial time: 15 seconds.

Maximum time: 600 seconds.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The LDP back-off delay time is a mechanism to prevent an endless sequence of session setup failures that occur between two LSRs with incompatible settings.

Example

This example shows how to configure the initial and maximum back-off delay time to 100 and 200 seconds.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# backoff 100 200
Switch(config-ldp)#
```

67-2 class map cos-exp

This command is used to configure the Class of Service (CoS) to the Experimental bits (EXP) mapping of the policy. Use the **no** command to remove the setting.

class map cos-exp *COS-LIST* **to** *EXP-VALUE*

no class map cos-exp [*COS-LIST***]**

Parameters

COS-LIST **to** *EXP-VALUE*	Specifies the list of CoS values to an EXP value. The series of CoS values can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after.
COS-LIST	Specifies the CoS list.

Default

None.

Command Mode

MPLS QoS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The CoS to EXP map is used to map an internal CoS value to an EXP value in the encapsulation of the label header.

Example

This example shows how to configure the CoS to EXP map in MPLS QoS “policy1”.

```
Switch# configure terminal
Switch(config)# mpls qos policy policy1
Switch(config-mpls-qos)# class map cos-exp 0 to 0
Switch(config-mpls-qos)# class map cos-exp 1 to 1
Switch(config-mpls-qos)# class map cos-exp 2 to 2
Switch(config-mpls-qos)# class map cos-exp 3 to 3
Switch(config-mpls-qos)# class map cos-exp 4 to 4
Switch(config-mpls-qos)# class map cos-exp 5 to 5
Switch(config-mpls-qos)# class map cos-exp 6,7 to 6
Switch(config-mpls-qos)#
```

67-3 class map exp-cos

This command is used to configure the class EXP to CoS mapping of the policy. Use the **no** command to remove the setting.

class map exp-cos *EXP-LIST* **to** *COS-VALUE*

no class map exp-cos [*EXP-LIST***]**

Parameters

EXP-LIST **to** *COS-VALUE*	Specifies the list of EXPs to be mapped to a CoS value. The range of EXP is from 0 to 7. The series of EXPs can be separated by commas (,) or hyphens (-) with no spaces or hyphens before and after.
EXP-LIST	Specifies the EXP list.

Default

Default EXP to CoS map:

- CoS: 0 1 2 3 4 5 6 7
- EXP: 2 0 1 3 4 5 6 7

Command Mode

MPLS QoS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The EXP to CoS map is used to map an EXP value in the encapsulation of the label header to an internal CoS value.

Example

This example shows how to configure the EXP to CoS map in MPLS QoS “policy1”.

```
Switch# configure terminal
Switch(config)# mpls qos policy policy1
Switch(config-mpls-qos)# class map exp-cos 0,2-7 to 3
Switch(config-mpls-qos)# class map exp-cos 1 to 6
Switch(config-mpls-qos)#
```

67-4 clear mpls ldp neighbor

This command is used to clear LDP neighbor sessions.

clear mpls ldp neighbor {all | *IP-ADDRESS***}**

Parameters

all	Specifies to clear all neighbors.
IP-ADDRESS	Specifies the IP address which is used as the peer LSR ID.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear LDP neighbor sessions.

Example

This example shows how to clear all LDP neighbors.

```
Switch# clear mpls ldp neighbor all
Switch#
```

67-5 discovery hello

This command is used to configure the LDP link hello hold-time and hello interval. Use the **no** form of this command to restore the default value.

discovery hello {holdtime *SECONDS* **| interval** *SECONDS***}**

no discovery hello {holdtime | interval}

Parameters

holdtime *SECONDS*	Specifies the link hello hold-time in seconds. The range is from 5 to 65535 seconds.
interval *SECONDS*	Specifies the link hello interval time in seconds. The range is from 1 to 65535 seconds.

Default

Hold time: 15 seconds.

Interval: 5 seconds.

Command Mode

Interface Configuration Mode.

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

LDP sends link hello messages at the configured interval to discover the neighbor. For a discovered neighbor, LDP maintains a hold-timer. The neighbor is timed out if the timer expired without the receipt of a hello message from the neighbor.

If the command is not configured for an interface, the global setting takes effect. If it is configured for an interface, the interface setting takes effect.

Example

This example shows how to configure the hello hold-time to 30 seconds and the hello interval to 10 seconds.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# discovery hello holdtime 30
Switch(config-ldp)# discovery hello interval 10
Switch(config-ldp)#
```

67-6 discovery targeted-hello accept

This command is used to enable the targeted hello message acceptance. Use the **no** form of this command to disable the targeted hello message acceptance.

discovery targeted-hello accept

no discovery targeted-hello accept

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If targeted hello message acceptance is disabled in the interface, and if the received targeted hello is not coming from the local configured targeted peer, the message will be ignored.

If targeted hello message acceptance is enabled in the interface, LSR will honor the received targeted hello messages sent by all neighbors.

Example

This example shows how to accept the targeted hello message.

```
Switch# configure terminal
Switch(config)# interface vlan 10
Switch(config-if)# discovery targeted-hello accept
Switch(config-if)#
```

67-7 discovery targeted-hello

This command is used to configure the LDP hello hold-time and hello interval for sessions to the targeted peer. Use the **no** form of this command to restore the default value.

discovery targeted-hello {holdtime *SECONDS* **| interval** *SECONDS***}**

no discovery targeted-hello {holdtime | interval}

Parameters

holdtime	Specifies the hold-time of the hello messages for sessions with extended peers. The range of is from 15 to 65535.
interval	Specifies the interval to the hello message for sessions with extended peers. The range is from 5 to 65535.

Default

Hold-time: 45 seconds.

Interval: 15 seconds.

Command Mode

LDP Target Peer Mode.

Command Default Level

Level: 12.

Usage Guideline

LDP sends the targeted hello message at the configured interval to discover the neighbor. For a discovered neighbor, LDP maintains a hold-timer. The neighbor will time out if the timer has expired without the receipt of a hello message from the neighbor.

Example

This example shows how to configure the LDP extended discovery hello hold-time to 90 seconds and interval to 30 seconds.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# neighbor 110.10.10.1 targeted
Switch(config-ldp-targeted-peer)# discovery targeted-hello holdtime 90
Switch(config-ldp-targeted-peer)# discovery targeted-hello interval 30
Switch(config-ldp-targeted-peer)#
```

67-8 discovery transport-address

This command is used to configure the transport address. Use the **no** form of this command to remove the transport address setting.

discovery transport-address {interface | *IP-ADDRESS***}**

no discovery transport-address

Parameters

interface	Specifies to use the IP address of the corresponding interface as the transmission address for the session on each interface.
IP-ADDRESS	Specifies to use the specified IP address as the transmission address uniformly.

Default

By default, the LSR ID is used as the transport address.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the LDP transport address. The transport address is used to establish a LDP TCP connection. By default, the LSR ID is used as the transport address by all interfaces. If you configure the transport address to **interface**, the IP address of each interface is used as the transport address. If you configure the transport address to a specified IP address, this address is used as transport address by all interfaces.

Example

This example shows how to configure the transport address to 192.168.0.1.

```
Switch# configure terminal
```

```
Switch(config)# mpls ldp configuration
Switch(config-ldp)# discovery transport-address 192.168.0.1
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-9 distribution-mode

This command is used to configure the label distribution mode. Use the **no** form of this command to restore the default value.

distribution-mode {dod | du}

no distribution-mode

Parameters

dod	Specifies the downstream on-demand distribution mode.
du	Specifies the downstream unsolicited distribution mode.

Default

By default, the distribution mode is downstream unsolicited.

Command Mode

Interface Configuration Mode.

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the mode is configured as Downstream-on-Demand mode, the downstream LSR advertises a label mapping when an upstream connection makes an explicit request. If the mode is configured as Downstream-Unsolicited mode, the downstream LSR advertises a label mapping when a label is learned in the routing table. If the command is not configured for an interface, the global setting takes effect. If it is configured for an interface, the interface setting takes effect.

Example

This example shows how to configure the label distribution mode to Downstream Unsolicited.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# distribution-mode du
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-10 explicit-null

This command is used to advertise the explicit null label to the penultimate hop. Use the **no** form of this command to reset to default setting.

explicit-null

no explicit-null

Parameters

None.

Default

By default, this option is Implicit null.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the egress router to configure the Penultimate Hop Popping (PHP) behavior of the upstream router. If the egress router advertises the Implicit Null label, the upstream will do Penultimate Hop Popping. If the egress router advertises the Explicit Null label, the upstream will keep the outer label without popping.

Example

This example shows how to configure the egress LSR advertise Explicit NULL label.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# explicit-null
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-11 keepalive-holdtime

This command is used to configure the keep-alive hold-time for LDP sessions. Use the **no** form of this command to restore the default value.

keepalive-holdtime *SECONDS*

no keepalive-holdtime

Parameters

SECONDS	Specifies the keep-alive hold-time in seconds. The range is from 15 to 65535 seconds.

Default

By default, this value is 40 seconds.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the LDP session keep-alive hold-time. LDP maintains a keep-alive hold timer for each peer session. If the keep-alive hold timer expires without receipt of an LDP PDU from the peer, LDP terminates the LDP session. Each LSR sends keep-alive messages at regular intervals to its LDP peers to keep the sessions active. The keep-alive interval is one third of the keep-alive hold-time.

Example

This example shows how to configure the keep-alive hold-time to 60 seconds.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# keepalive-holdtime 60
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-12 label-retention-mode

This command is used to configure the label retention mode. Use the **no** form of this command to restore the default value.

label-retention-mode {liberal | conservative}

no label-retention-mode

Parameters

liberal	Specifies the liberal label retention mode.
conservative	Specifies the conservative label retention mode.

Default

By default the label retention mode is configured as liberal.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the label distribution method is Downstream-Unsolicited and the label retention mode is conservative, once the LSR received label bindings from LSRs which are not its next hop for that FEC, it discards such bindings. If the label retention mode is liberal, it maintains such bindings. It helps to speed up the setup of LSP in case there is a change in the next hop.

Example

This example shows how to configure the label retention mode to conservative.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# label-retention-mode conservative
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-13 loop-detection

This command is used to enable loop detection. Use the **no** form of this command to disable loop detection.

loop-detection

no loop-detection

Parameters

None.

Default

By default, this option is disabled.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable LDP loop detection. LDP loop detection makes use of the Path Vector and Hop Count TLVs carried by the label request and label mapping messages to prevent looping of LDP messages. If enabled, LDP does not send the LDP message that violates the path vector check or hop count check to next hop.

Example

This example shows how to enable LDP loop detection.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# loop-detection
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-14 lsp-control-mode

This command is used to configure the Label-Switched Path (LSP) control mode. Use the **no** form of this command to restore the default value.

lsp-control-mode {independent | ordered}

no lsp-control-mode

Parameters

independent	Specifies the independent control mode.
ordered	Specifies the ordered control mode.

Default

By default, the LSP control mode is configured as independent.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In Independent LSP Control, each Label Switching Router (LSR) independently binds a label to a Forwarding Equivalence Class (FEC) and distributes the binding to its label distribution peers. In Ordered LSP Control, an LSR only binds a label to a FEC if it is the egress LSR for that FEC, or if it has already received a label binding for that FEC from its next hop for that FEC.

Example

This example shows how to configure the LSP control mode to ordered.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# lsp-control-mode ordered
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-15 lsp trigger

This command is used to configure an LSP trigger filter rule. Use the **no** form of this command to remove the rule.

lsp trigger [*SN***] {permit | deny} {ip** *NETWORK-PREFIXIPREFIX-LENGTH* **| any}**

no lsp trigger {all | *SN***}**

Parameters

SN	(Optional) Specifies the sequence number of the LSP trigger filter rule. When creating a new rule, if not specified, the SN begins from 10 and is incremented by 10. The SN range is from 1 to 10000.
permit	Specifies to permit LDP in establishing the LSP to follow the IP prefix FEC.
deny	Specifies no permit LDP in establishing the LSP to follow the IP prefix FEC.
ip *NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the IP prefix FEC on which the rule will apply.
any	Specifies that the rule will apply on any IP prefix FEC.
all	Specifies to delete all LSP trigger filters.

Default

None.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure LSP trigger filter rules. The LSP trigger filter rules are IP access list rules that it is used to control the IP routes that can be used to trigger the establishment of an LSP. For example, if there are two routes for 172.18.1.0/24 and 172.18.2.0/24, the LSP trigger filter permits 172.18.1.0/24 and denies 172.18.2.0/24. The switch can only establish an LSP for 172.18.1.0/24.

Example

This example shows how to create LSP trigger filter rules that permit establishing the LSP for 192.1.1.0/24 and not to permit establishing LSP for other routes.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# lsp trigger 10 permit ip 192.1.1.0/24
Switch(config-ldp)# lsp trigger 20 deny any
Switch(config-ldp)#
```

67-16 maxhops

This command is used to configure the maximum number of hops permitted in the LSP setup. Use the **no** form of this command to restore the default value.

maxhops *VALUE*

no maxhops

Parameters

VALUE	Specifies the maximum number of hops permitted in the LSP setup. The range is from 1 to 255

Default

By default, this value is 254.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the maximum hop count limitation command to prevent looping of the LDP mapping message or label of request message during routing transitions. If loop detection is enabled, LDP does not send the LDP message that violates the maximum hop limitation to the next hop.

Example

This example shows how to configure the maximum hop count to 30.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# maxhops 30
Warning: The configuring will lead to LDP sessions restart.
```

```
Switch(config-ldp)#
```

67-17 match

This command is used to apply the policy to FECs. Use the **no** command to remove the setting.

match {ip *NETWORK-PREFIXIPREFIX-LENGTH* **| vc** *IP-ADDRESS VC-ID***}**

no match {all | ip *NETWORK-PREFIXIPREFIX-LENGTH* **| vc** *IP-ADDRESS VC-ID***}**

Parameters

ip *NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the IP prefix FEC.
vc *IP-ADDRESS VC-ID*	Specifies the VC FEC.
all	Specifies to remove all binding FECs of the policy.

Default

By default, this option is disabled.

Command Mode

MPLS QoS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to apply a MPLS QoS policy to FECs. The QoS policy will be applied to all MPLS packets of the FEC. A FEC can only be bound to at most one policy.

Example

This example shows how to apply the MPLS QoS “policy1” to FEC 172.18.1.0/24.

```
Switch# configure terminal
Switch(config)# mpls qos policy policy1
Switch(config-mpls-qos)# match ip 172.18.1.0/24
Switch(config-mpls-qos)#
```

67-18 md5 authentication

This command is used to enable the LDP authentication. Use the **no** form of this command to restore the default value.

md5 authentication

no md5 authentication

Parameters

None.

Default

By default, this option is disabled.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable LDP authentication. If the LDP MD5 authentication is enabled, the LSR applies the MD5 algorithm to compute the MD5 digest for the TCP segment that will be sent to the peer. This computation makes use of the peer password as well as the TCP segment. When the LSR receives a TCP segment with an MD5 digest, it validates the segment by calculating the MD5 digest (using its own record of the password) and compares the computed digest with the received digest. If the comparison fails, the segment is dropped without any response to the sender. The LSR ignores LDP Hellos from any LSR for which a password has not been configured.

Example

This example shows how to enable LDP MD5 authentication.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# md5 authentication
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-19 mpls ip

This command is used, in the global configuration mode, to enable the MPLS forwarding globally. This command is used, in the interface configuration mode, to enable the MPLS forwarding on an interface. Use the **no** form of the command to disable MPLS forwarding.

mpls ip

no mpls ip

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to start MPLS forwarding on an interface. Both the global setting and per interface MPLS setting need to be enabled.

Example

This example shows how to enable MPLS globally and enable MPLS on VLAN 100.

```
Switch# configure terminal
Switch(config)# mpls ip
Switch(config)# interface vlan100
Switch(config-if)# mpls ip
Switch(config-if)#
```

67-20 mpls label protocol ldp

This command is used, in the interface configuration mode, to enable LDP on this interface. This command is used, in the global configuration mode, to enable LDP globally. Use the **no** command to disable LDP.

mpls label protocol ldp

no mpls label protocol ldp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

LDP is running on an interface only when:

- MPLS and LDP are globally enabled.
- MPLS and LDP are enabled on this interface.

Example

This example shows how to enable LDP globally and enable LDP on VLAN 100.

```
Switch# configure terminal
Switch(config)# mpls label protocol ldp
Switch(config)# interface vlan 100
Switch(config-if)# mpls label protocol ldp
Switch(config-if)#
```

67-21 mpls ldp configuration

This command is used to enter the LDP configuration mode to configure LDP related settings.

mpls ldp configuration

Parameters

None.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to enter the LDP configuration mode to configure LDP related settings.

Example

This example shows how to enter the LDP configuration mode.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)#
```

67-22 mpls qos policy

This command is used to enter the MPLS QoS configuration mode. If the policy doesn't exist, a new policy will be created. Use **no** command to remove the policy.

mpls qos policy *NAME*

no mpls qos policy {all | *NAME***}**

Parameters

NAME	Specifies the MPLS QoS policy name. The maximum name length is 32 characters.
all	Specifies to remove all MPLS QoS policies.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the MPLS QoS configuration mode. If the policy doesn't exist, a new policy will be created. The MPLS QoS policy can be applied to MPLS FECs. Use the **class-map exp-cos**

command to set the mapping from EXP to priority for incoming MPLS packets. The inbound EXP CoS mapping takes effect only when trust EXP is enabled.

Use the **class-map cos-exp** command to set the mapping table for mapping from CoS to EXP for packets outbound to MPLS network. Only one mapping table can be specified for each direction. The command issued later overwrites the previous setting.

Once MPLS packets are received and if there is inbound an EXP to CoS mapping entry for the FEC, the device assigns CoS according to the inbound EXP. Otherwise, the CoS is assigned according to 802.1p. If the incoming packet is tagged, the priority is used from its tag. Otherwise, use the CoS from the port's default priority.

The device selects the CoS queue according to the CoS to CoS queue mapping rule.

When the device transmits packets to the outgoing interface, if there is outbound CoS-EXP mapping table, the EXP will always inherit the settings according to the mapping table. Otherwise, if the incoming packets have an MPLS label, the EXP will not be modified. If the incoming packets are not MPLS packets, the EXP will be set to zero.

Example

This example shows how to create an MPLS QoS policy called "policy1".

```
Switch# configure terminal
Switch(config)# mpls qos policy policy1
Switch(config-mpls-qos)#
```

67-23 mpls static ftn

This command is used to add a static FEC–To-NHLFE Map (FTN) entry. NHLFE stands for Next Hop Label Forwarding Entry. Use the **no** command to remove the previous configured static FTN.

mpls static ftn *NETWORK-PREFIX*|*PREFIX-LENGTH* **out-label** *LABEL-VALUE* **nexthop** *IP-ADDRESS*

no mpls static ftn {all | *NETWORK-PREFIX*|*PREFIX-LENGTH***}**

Parameters

NETWORK-PREFIX|*PREFIX-LENGTH*	Specifies the FEC of the static FTN.
out-label *LABEL-VALUE*	Specifies the out-label of this FEC.
nexthop *IP-ADDRESS*	Specifies the next-hop IP address of this FEC.
all	Specifies to delete all static FTN LSPs.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to add a static FTN entry. At the ingress Label Edge Router (LER), the incoming IP packets that are classified to the Forwarding Equivalence Class (FEC) will be pushed with the MPLS label and forwarded to the next hop according to the FEC-to-NHLFE (FTN).

Example

This example shows how to configure a static FTN that pushes the label 100 for prefix FEC 172.18.10.0/24.

```
Switch# configure terminal
Switch(config)# mpls static ftn 172.18.10.0/24 out-label 100 nexthop 110.1.1.2
Switch(config)#
```

67-24 mpls static ilm

This command is used to add a static Incoming Label Map (ILM) entry. Use the **no** command to remove the previous configured ILM.

mpls static ilm in-label *LABEL-VALUE* **forward-action {swap-label** *LABEL-VALUE* **| pop} nexthop** *IP-ADDRESS* **fec** *NETWORK-PREFIXIPREFIX-LENGTH*

no mpls static ilm {all | in-label *LABEL-VALUE***}**

Parameters

in-label *LABEL-VALUE*	Specifies the incoming label value of the ILM.
forward-action	Specifies the forward behavior of this ILM entry. **swap-label:** Specifies to swap the top label in the label stack and forward the MPLS packets to next-hop. **pop:** Specifies to pop the top label in the label stack and forward the MPLS packets to next-hop.
swap-label *LABEL-VALUE*	Specifies the swapped outgoing label value.
nexthop *IP-ADDRESS*	Specifies the next-hop IP address of this FEC.
fec *NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the IP prefix FEC that is associated with the ILM.
all	Specifies to delete all static ILM LSP.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to add a static ILM entry. At LSR, the incoming MPLS packets that are matched to the incoming label will be processed according configured ILM action. The label operation is either swapping the incoming top label to configured outgoing label or popping the top label and then forwards the packets to the next-hop.

Example

This example shows how to configure a static ILM that swaps the label from 100 to 200 for the prefix FEC 172.18.10.0/24 at the transit LSR.

```
Switch# configure terminal
Switch(config)# mpls static ilm in-label 100 forward-action swap-label 200 nexthop
120.1.1.3 fec 172.18.10.0/24
Switch(config)#
```

This example shows how to configure a static ILM that pops the label from 100 for prefix FEC 172.18.10.0/24 at the egress LER.

```
Switch# configure terminal
Switch(config)# mpls static ilm in-label 100 forward-action pop nexthop 120.1.1.3 fec
172.18.10.0/24
Switch(config)#
```

67-25 neighbor password

This command is used to configure an LDP peer password. Use the **no** form of this command to restore the default value.

neighbor *IP-ADDRESS* **password** *PASSWORD*

no neighbor *IP-ADDRESS* **password**

Parameters

IP-ADDRESS	Specifies the peer IP address. The IP address will be the peer's LSR ID.
PASSWORD	Specifies the password in the clear text form.

Default

By default, a peer has no password.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure an LDP peer password. If the MD5 authentication is enabled, the LSR only establishes sessions with the peer when they exchange the same password. The password setting will be applied to negotiation with link neighbors or targeted neighbors.

Example

This example shows how to enable MD5 authentication and configure the peer 10.90.90.12 password to "abcd".

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# md5 authentication
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)# neighbor 10.90.90.12 password abcd
```

```
Warning: The configuring will lead to the LDP session of the peer restart.
Switch(config-ldp)#
```

67-26 neighbor targeted

This command is used to create an LDP targeted peer. Use the **no** form of this command to remove a configured LDP targeted peer.

neighbor *IP-ADDRESS* **targeted**

no neighbor *IP-ADDRESS* **targeted**

Parameters

IP-ADDRESS	Specifies the LSR ID of the targeted peer.

Default

None.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a targeted peer. The targeted peer is used to establish the LDP session with the non-directly connected neighbor.

Example

This example shows how to create a targeted peer 110.10.10.1.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# neighbor 110.10.10.1 targeted
Switch(config-ldp-targeted-peer)#
```

67-27 path-vector maxlength

This command is used to configure the maximum path vector length. Use the **no** form of this command to restore the default value.

path-vector maxlength *VALUE*

no path-vector maxlength

Parameters

VALUE	Specifies the maximum path vector length. The range is from 1 to 255.

Default

By default, this value is 254.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If loop detection is enabled, the LDR ID that is in the path vector list of the label mapping message or the label request message or the path vector length exceeds the maximum length, then it is deemed that a loop occurs.

Example

This example shows how to configure the maximum path vector to 30.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# path-vector maxlength 30
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-28 ping mpls ipv4

This command is used to check the connectivity of the LSP for the specified FEC.

ping mpls ipv4 *NETWORK-PREFIXIPREFIX-LENGTH* **[repeat** *COUNT***] [timeout** *SECONDS***]**

Parameters

NETWORK-PREFIXIPREFIX-LENGTH	Specifies the IPv4 prefix FEC whose LSP connectivity will be checked.
repeat *COUNT*	Specifies the number of times to send the same packet. This value must be between 1 and 255. The default value is 4.
timeout *SECONDS*	Specifies the interval in seconds to send the MPLS request packet. This value must be between 1 and 99 seconds. The default value is 2 seconds.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to check the connectivity of the LSP for the specified FEC. If there is no LSP for the specified FEC, the “Destination unreachable” message will be displayed. Otherwise, MPLS echo request messages will be sent out to along with the LSP of the specified FEC. If the egress LSR received the request message, it will reply the request message sender with an MPLS echo reply message. If the sender cannot receive replies before the timeout, the “Request timed out” message will be displayed.

Example

This example shows how to check the connectivity of the LSP for network 192.1.1.0/24.

```
Switch# ping mpls ipv4 192.1.1.0/24

Reply from 192.1.1.1, time<10ms
Reply from 192.1.1.1, time<10ms
Reply from 192.1.1.1, time<10ms
Reply from 192.1.1.1, time<10ms

Ping Statistics for 192.1.1.0/24
Packets: Sent =4, Received =4, Lost =0

Switch#
```

This example shows how to check the connectivity of the LSP for network 110.1.1.0/24.

```
Switch# ping mpls ipv4 110.1.1.0/24

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping Statistics for FEC 110.1.1.0/24
Packets: Sent =4, Received =0, Lost =4

Switch#
```

67-29 router-id

This command is used to configure the LSR ID of the LDP. Use the **no** command to restore the LSR ID to the default value.

router-id *IP-ADDRESS*

no router-id

Parameters

IP-ADDRESS	Specifies the IPv4 address that will be used as the LSR ID. The IPv4 address must be an IP address of an existing interface.

Default

None.

Command Mode

LDP Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The LSR ID is used to identify the LSR in the MPLS network. It is recommended to set the LSR ID to the IP address of a loopback interface. If the command is not configured, by default, the LDP will automatically select the router ID. If LDP is running, the LSR ID will not be automatically changed.

The value of the LSR ID should be unique. By default, the LSR ID is used as the transport address. It is necessary to ensure the LSR ID is route reachable for other LSRs.

Example

This example shows how to configure the LDP LSR ID to 110.10.10.30.

```
Switch# configure terminal
Switch(config)# mpls ldp configuration
Switch(config-ldp)# router-id 110.10.10.30
Warning: The configuring will lead to LDP sessions restart.
Switch(config-ldp)#
```

67-30 show mpls

This command is used to display the MPLS settings or MPLS interfaces' status.

show mpls [interface [*INTERFACE-ID***]]**

Parameters

interface	Specifies to display the MPLS interface's status.
INTERFACE-ID	(Optional) Specifies the interface that will be displayed. If not specified, all MPLS interfaces' information will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MPLS settings or MPLS interfaces' status.

Example

This example shows how to display an MPLS interface's status.

```
Switch# show mpls interface

Interface  IP Address      Oper Status
---------  -------------   ------------
VLAN 10    10.90.90.1/24   UP
VLAN 20    172.18.1.1/24   Down

Total Entries: 2
```

```
Switch#
```

This example shows how to display the MPLS's global settings.

```
Switch# show mpls

MPLS Status       : Enabled
LSP Trap Status   : Disabled

Switch#
```

67-31 show mpls forwarding-table

This command is used to display the MPLS label forwarding path information.

show mpls forwarding-table [ip *NETWORK-PREFIXIPREFIX-LENGTH***] [detail]**

Parameters

ip *NETWORK-PREFIXIPREFIX-LENGTH*	(Optional) Specifies the IP prefix FEC. If not specified, display all FECs.
detail	Specifies to display detailed information of the MPLS label forwarding path information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the MPLS forwarding path information.

Example

This example shows how to display all MPLS label forwarding path information.

```
Switch# Show mpls forwarding-table

LSP  FEC            In Label  Out Label   Out Interface   Next Hop
---- -------------  --------  ---------   -------------   ---------------
1   201.1.1.0/24   1020      1030          VLAN 10         172.18.1.1
2   201.2.1.0/24   1060      1040          VLAN 20         192.1.1.2
3   172.1.1.1/32   1050      -             VLAN 10         172.18.1.1
4   192.1.1.0/24   -         1070          VLAN 10         172.18.1.1

Total Entries: 4

Switch#
```

This example shows how to display all detailed MPLS label forwarding path information.

```
Switch# Show mpls forwarding-table detail

LSP: 1
Type: Transit          Status: Up
FEC: 201.1.1.0/24      Owner: LDP
In Label: 1020         Out Label: Swap 1030
Next Hop: 172.18.1.1   Out Interface: VLAN 10

LSP: 2
Type: Transit          Status: Up
FEC: 201.2.1.0/24      Owner: LDP
In Label: 1060         Out Label: Swap 1040
Next Hop: 192.1.1.2    Out Interface: VLAN 20

LSP: 3
Type: Egress           Status: Up
FEC: 172.1.1.1/32      Owner: LDP
In Label: 1050         Out Label: Pop
Next Hop: 172.18.1.1   Out Interface: VLAN 10

LSP: 4
Type: Ingress          Status: Up
FEC: 192.1.1.0/24      Owner: LDP
In Label: -            Out Label: Push 1070
Next Hop: 172.18.1.1   Out Interface: VLAN 10

LSP: 5
Type: Ingress          Status: Up
FEC: VC11/192.1.1.1    Owner: LDP
In Label: -            Out Label: Push 1100/1070
Next Hop: 172.18.1.1   Out Interface: VLAN 10

LSP: 6
Type: Egress           Status: Up
FEC: VC11/192.1.1.1    Owner: LDP
In Label: 1200         Out Label: Pop

Total Entries: 6

Switch#
```

67-32 show mpls ldp bindings

This command is used to display all LDP label binding information.

show mpls ldp bindings

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all LDP label binding information.

Example

This example shows how to display all LDP label binding information.

```
Switch# show mpls ldp bindings

  FEC: 3.3.3.3/32
     State     : Established
     In-lable  : 0
     Upstream  : 2.2.2.2
     Out-lable : None
     Downstream: None
  FEC: 1.1.1.1/32
     State     : Established
     In-lable  : None
     Upstream  : None
     Out-lable : 172
     Downstream: 2.2.2.2

 Total Entries: 2

Switch#
```

67-33 show mpls ldp discovery

This command is used to display LDP peer information.

show mpls ldp discovery

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the interfaces on which LDP neighbor has been discovered.

Example

This example shows how to display all MPLS LDP neighbors.

```
Switch# show mpls ldp discovery

 Local LDP Identifier: 10.1.1.1:0
 Discovery Sources:
   Interfaces:
     VLAN 10 (ldp): xmit/recv
        LDP Id: 172.23.0.77:0
     VLAN 20 (ldp): xmit/recv
        LDP Id: 192.18.0.15:0
   Targeted Hellos:
     10.1.1.1 -> 10.133.0.33 (ldp): active, xmit/recv
        LDP Id: 10.133.0.33:0
     10.1.1.1 -> 172.18.30.2 (ldp): passive, xmit/recv
        LDP Id: 172.18.30.2:0

Switch#
```

67-34 show mpls ldp information

This command is used to display LDP global information.

show mpls ldp information

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display LDP global information.

Example

This example shows how to display LDP global information.

```
Switch# show mpls ldp information

 LSR ID                 : 3.3.3.3
 LDP Version            : 1.0
 LDP State              : Enabled
```

```
 TCP Port               : 646
 UDP Port               : 646
 Max PDU Length         : 1500
 Initial Backoff        : 15 Seconds
 Max Backoff            : 600 Seconds
 Transport Address      : 3.3.3.3
 Keep Alive Time        : 60 Seconds
 Link Hello Holdtime    : 15 Seconds
 Link Hello Interval    : 5 Seconds
 Distribution Method    : DU
 LSP Control Mode       : Ordered
 Label Retention        : Conservative
 Loop Detection         : Enabled
 Path Vector Limit      : 254
 Hop Count Limit        : 30
 Authentication         : Disabled
 PHP                    : Explicit null
 Trap Status            : Disabled

Switch#
```

67-35 show mpls ldp interface

This command is used to display LDP interface information.

show mpls ldp interface [*INTERFACE-ID***]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface that will be displayed. If not specified, all interfaces' information will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display LDP information on the interface.

Example

This example shows how to display LDP information on all interfaces.

```
Switch# show mpls ldp interface

Interface: if1
---------------------------------------
Admin State           : Enabled
```

```
Oper State            : Disabled
Targeted Hello Accept : Acceptable
Hello Interval        : 5(Sec)
Hello Hold Time       : 15(Sec)
Distribution Method   : DoD

Interface: if2
---------------------------------------
Admin State           : Enabled
Oper State            : Disabled
Targeted Hello Accept : Acceptable
Hello Interval        : 5(Sec)
Hello Hold Time       : 15(Sec)
Distribution Method   : DoD

Total Entries: 2

Switch#
```

67-36 show mpls ldp neighbor

This command is used to display LDP peer information.

show mpls ldp neighbor [*IP-ADDRESS***]**

Parameters

IP-ADDRESS	Specifies the IP address used as the peer LSR ID. If not specified, all neighbors will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all peers learned by LDP.

Example

This example shows how to display all LDP neighbors.

```
Switch# show mpls ldp neighbor

Peer : 202.11.1.1:0
 ---------------------------------------
Protocol Version    : 1.0
 Transport address   : 202.11.1.1
 Keep Alive Time     : 40 (sec)
```

```
 Distribution Method : DU
 Loop Detect         : Disabled
 Path Vector Limit   : 0
 Max PDU Length      : 1500

 Peer : 192.1.1.1:0
 ------------------------------------
 Protocol Version    : 1.0
 Transport address   : 192.1.1.1
 Keep Alive Time     : 40 (sec)
 Distribution Method : DU
 Loop Detect         : Disabled
 Path Vector Limit   : 1500
 Max PDU Length      : 0

 Peer : 202.20.1.1:0
 ------------------------------------
 Protocol Version    : 1.0
 Transport address   : 202.20.1.1
 Keep Alive Time     : 40 (sec)
 Distribution Method : DU
 Loop Detect         : Disabled
 Path Vector Limit   : 0
 Max PDU Length      : 1500

Total Entries : 3

Switch#
```

67-37 show mpls ldp neighbor password

This command is used to display the LDP neighbor password.

show mpls ldp neighbor password

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all LDP neighbor password configurations.

Example

This example shows how to display LDP neighbors' password configurations.

```
Switch# show mpls ldp neighbor password

Neighbor        Password
------------    ----------
202.11.1.1      123456
192.1.1.1       abcd

Total Entries : 2

Switch#
```

67-38 show mpls ldp neighbor targeted

This command is used to display the LDP targeted peer configuration.

show mpls ldp neighbor targeted

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all LDP targeted peer configurations.

Example

This example shows how to display all LDP targeted peer configurations.

```
Switch# show mpls ldp neighbor targeted

Targeted Peer  Hello Interval   Hold Time
-------------  --------------   -----------
192.10.1.1     15(Sec)          45(Sec)
192.10.1.2     15(Sec)          45(Sec)

Total Entries : 2

Switch#
```

67-39 show mpls ldp session

This command is used to display LDP session information.

show mpls ldp session [peer *IP-ADDRESS***] [detail | statistic]**

Parameters

peer *IP-ADDRESS*	Specifies the IP address of the peer LSR ID. If not specified, all sessions will be displayed.
detail	Specifies to display detailed information.
statistic	Specifies to display session statistics.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all LDP sessions.

Example

This example shows how to display all LDP session information.

```
Switch# show mpls ldp session

Peer        Status        Role      Keep Alive  Distribution Method
----------  ------------  --------  ----------- ------------------
10.1.1.2:0  OPERATIONAL   Active    40(Sec)      DU
20.1.1.2:0  OPERATIONAL   Passive   40(Sec)      DU

Total Entries : 2

Switch#
```

This example shows how to display LDP session detailed information of peer 10.1.1.2.

```
Switch# show mpls ldp session peer 10.1.1.2 detail

Peer                 : 10.1.1.2:0
Status              : OPERATIONAL
Role                : Active
Keep Alive(Sec)     : 40
Remain Time(Sec)    : 20
Create Time         : 2013-12-1 14:10:30
Distribution Method : DU
Loop Detection      : Enabled
Max PDU Length      : 1500
Address List        : 10.1.1.2
                      172.18.1.1

Total Entries: 1
```

```
Switch#
```

This example shows how to display LDP session statistics for peer 10.1.1.2.

```
Switch# show mpls ldp session peer 10.1.1.2 statistic

Peer 10.1.1.2
-----------------------------------------
Notification Message       : TX 10/RX 2
Initialization Message     : TX 2/RX 2
Keep Alive Message         : TX 100/RX 100
Address Message            : TX 1/RX 1
Address Withdraw Message   : TX 0/RX 0
Label Mapping Message      : TX 2/RX 1
Label Request Message      : TX 2/RX 1
Label Withdraw Message     : TX 0/RX 0
Label Release Message      : TX 0/RX 0
Label Abort Message        : TX 0/RX 0

Total Entries: 1

Switch#
```

67-40 show mpls ldp statistic

This command is used to display LDP global statistic information.

show mpls ldp statistic

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display LDP global statistic information.

Example

This example shows how to display LDP global statistic information.

```
Switch# show mpls ldp statistic

SessionAttempts              :  0
SessionRejectedNoHelloErrors :  0
```

```
SessionRejectedAdErrors      :  0
SessionRejectedMaxPduErrors  :  0
SessionRejectedLRErrors      :  0
BadLdpIdentifierErrors       :  0
BadPduLengthErrors           :  0
BadMessageLengthErrors       :  0
BadTlvLengthErrors           :  0
MalformedTlvValueErrors      :  0
KeepAliveTimerExpErrors      :  0
ShutdownReceivedNotifications:  0
ShutdownSentNotifications    :  0

Switch#
```

67-41 show mpls lsp trigger

This command is used to display MPLS LSP trigger filter rule(s).

show mpls lsp trigger [*SN***]**

Parameters

SN	(Optional) Specifies the sequence number of the MPLS LSP trigger filter rule to be displayed. If not specified, all rules will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MPLS LSP trigger filter rule(s).

Example

This example shows how to display all MPLS LSP trigger filter rules.

```
Switch# show mpls lsp trigger

SN      Prefix FEC        Action
 -----   --------------    --------
10      192.1.1.0/24       Permit
20      Any                Deny

Total Entries : 2

Switch#
```

67-42 show mpls qos

This command is used to display MPLS QoS settings.

show mpls qos {policy [<*NAME*>] | ip *NETWORK-PREFIXIPREFIX-LENGTH* **| vc** *IP-ADDRESS VC-ID***}**

Parameters

policy	Specifies to display the MPLS QoS policy.
NAME	Specifies the MPLS QoS policy name.
ip *NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the IP prefix FEC whose QoS policy will be displayed.
vc *IP-ADDRESS VC-ID*	Specifies the VC FEC whose QoS policy will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the MPLS QoS policy settings.

Example

This example shows how to displays all MPLS QoS settings.

```
Switch# show mpls qos policy

MPLS QoS Policy: policy1, Trust EXP
  Inbound EXP to CoS:
      EXP : 0, 1, 2, 3, 4, 5, 6, 7
      CoS : 0, 1, 2, 3, 4, 5, 6, 6
  Outbound CoS to EXP:
      CoS : 0, 1, 2, 3, 4, 5, 6, 7
      EXP : 3, 6, 3, 3, 3, 3, 3, 3
  Binding FECs:
     172.18.1.0/24, 110.1.1.0/24

Total Entries: 1

Switch#
```

This example shows how to display the MPLS QoS setting for FEC 172.18.1.0/24.

```
Switch# show mpls qos ip 172.18.1.0/24

FEC 172.18.1.0/24 binding MPLS QoS policy: policy1
```

```
Switch#
```

67-43 snmp-server enable traps mpls ldp

This command is used to enable the LDP trap state. Use the **no** form of this command to disable the LDP trap state.

snmp-server enable traps mpls ldp

no snmp-server enable traps mpls ldp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command used to configure the LDP trap state.

Example

This example shows how to enable the LDP trap state.

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

67-44 snmp-server enable traps mpls lsp

This command is used to enable the MPLS LSP trap state. Use the **no** form of this command to disable the MPLS LSP trap state.

snmp-server enable traps mpls lsp

no snmp-server enable traps mpls lsp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command used to configure the MPLS LSP trap state.

Example

This example shows how to enable the MPLS LSP trap state.

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

67-45 traceroute mpls ipv4

This command is used to configure the hop-by-hop fault localization as well as the path tracing LSP for the specified FEC.

traceroute mpls ipv4 *NETWORK-PREFIXIPREFIX-LENGTH* **[timeout** *SECONDS***]**

Parameters

NETWORK-PREFIXIPREFIX-LENGTH	Specifies the IPv4 prefix FEC whose LSP connectivity will be checked.
timeout *SECONDS*	Specifies the interval in seconds to send the MPLS request packet. This value must be between 1 and 99 seconds. The default value is 2 seconds.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used for hop-by-hop fault localization as well as path tracing the LSP of the specified FEC. If there is no LSP for the specified FEC, the “Destination unreachable” message will be displayed. Otherwise, MPLS echo request messages will be sent out to along the LSP of the specified FEC. The TTL in the outmost label of the MPLS echo requests is set successively to 1, 2, 3, and so on. It forces the echo request expired at each successive LSR along the LSP. The LSR returns an MPLS echo reply. If the sender cannot receive a reply before the timeout, the trace route will stop.

Example

This example shows how to trace route the LSP for network 192.1.1.0/24.

```
Switch# traceroute mpls ipv4 192.1.1.0/24

Reply from 170.1.1.1, time<10ms
Reply from 200.1.2.3, time=20ms
Reply from 210.1.1.4, time=30ms
```

```
Reply from 192.1.1.1, time=40ms

Trace complete.

Switch#
```

This example shows how to trace route the LSP for network 110.1.1.0/24.

```
Switch# traceroute mpls ipv4 110.1.1.0/24

Reply from 170.1.1.1, time<10ms
Request timed out

Trace complete.

Switch#
```

67-46 trust exp

This command is used to trust the incoming label's top-most EXP as the priority. Use the **no** command to disable the trust.

trust exp

no trust exp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

MPLS QoS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to trust the incoming label's top-most EXP as the priority. If the EXP is trusted, the matched packets are scheduled according to the EXP to the priority mapping of the MPLS QoS policy. Otherwise, the packets are scheduled according to the 802.1p priority.

Example

This example shows how to enable trust EXP.

```
Switch# configure terminal
Switch(config)# mpls qos policy policy1
Switch(config-mpls-qos)# trust exp
Switch(config-mpls-qos)#
```

68. Neighbor Discovery (ND) Inspection Commands

68-1 ipv6 nd inspection policy

This command is used to create an ND inspection policy. This command will enter into 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an ND inspection policy. This command will enter into 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)#
```

68-2 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 the 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.

Command Default Level

Level: 12.

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)#
```

68-3 device-role

This command is used to specify the role of the attached device. Use the **no** form of the command to reset 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.

Command Default Level

Level: 12.

Usage Guideline

The command is used 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)#
```

68-4 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.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port and port channel configuration. The command is used to apply the ND Inspection policy on a specified interface. If **no policy-name** 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 interface eth1/0/3.

```
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)#
```

68-5 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the policy name is specified, only the specified policy information is displayed. If the policy name is not specified, information is displayed for all policies.

Example

This example shows how to display the policy configuration for a policy named “inspect1” and all the interfaces where the policy is applied:

```
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#
```

69. Network Access Authentication Commands

69-1 authentication guest-vlan

This command is used to configure the guest VLAN setting. Use the **no** form of the 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.

Command Default Level

Level: 12.

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 only 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)#
```

69-2 authentication host-mode

This command is used to specify the authentication mode. Use the **no** form of the command to reset to the default setting.

authentication host-mode {multi-host | multi-auth [vlan *VLAN-ID* **[, | -]]}**

no authentication host-mode [multi-auth vlan *VLAN-ID* **[, | -]]**

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 multi-auth mode. Each host will be authenticated individually.
vlan *VLAN-ID*	(Optional) Specifies the authentication VLAN(s). This is useful when different VLANs on the switch have different authentication requirements. Using the **no** command, all the VLANs are removed If not specified. This means that it does not care which VLAN the client comes from, the client will be authenticated if the client's MAC address (regardless of the VLAN) is not authenticated. After the client is authenticated, the client will not be re-authenticated when received from other VLANs. This option is useful for trunk ports to do per-VLAN authentication control. When a port's authentication mode is changed to multi-host, the previous authentication VLAN(s) on this port will be cleared.

Default

By default, **multi-auth** is used.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the port is operated in the **multi-host** mode, and if one of the hosts is authenticated, then 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, then 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 Ethernet port 1/0/1 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)#
```

69-3 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable periodic re-authentication for a port.

Example

This example shows how to enable periodic re-authentication on Ethernet port eth1/0/1.

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

69-4 authentication timer inactivity

This command is used to configure the timer after which an inactive session is terminated. Use the **no** form of the command to disable the inactivity timer

authentication timer inactivity {*SECONDS***}**

no authentication timer inactivity

Parameters

SECONDS	Specifies to configure the timer after which an inactive session is terminated. The range is from 120 to 65535.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the inactivity timer is configured, a user session will be terminated if the session sustains no activity for the configured period of time. If the inactivity timer is configured, it should be shorter than the timer value configured by authentication timer re-authentication command.

Example

This example shows how to configure the inactivity timer to 240 for eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication timer inactivity 240
Switch(config-if)#
```

69-5 authentication timer reauthentication

This command is used to configure the timer to re-authenticate a session. Use the **no** form of the command to revert the setting to default.

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.

Command Default Level

Level: 12.

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 eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication timer reauthentication 200
Switch(config-if)#
```

69-6 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 the command to revert the setting to default.

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.

Command Default Level

Level: 12.

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 eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# authentication timer restart 20
Switch(config-if)#
```

69-7 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 [0 | 7]** *PASSWORD* **[vlan** *VLAN-ID***]**

no authentication username *NAME* **[vlan]**

Parameters

NAME	Specifies the username with a maximum of 32 characters.
0	(Optional) Specifies the password in the clear text form. If neither 0 nor 7 are specified, the default form is clear text.
7	(Optional) Specifies the password in the encrypted form. If neither 0 nor 7 are specified, the default form is clear text.
password *STRING*	Specifies to set password for MAC authentication. If in the clear text form, the length of the string cannot be over 32.
vlan *VLAN-ID*	Specifies the VLAN to be assigned.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

69-8 clear authentication sessions

This command is used to remove authentication sessions.

clear authentication sessions {mac | wac | dot1x | all | interface *INTERFACE-ID* **[mac | wac | dot1x] | mac-address** *MAC-ADDRESS***}**

Parameters

mac	Specifies to clear all MAC sessions.
wac	Specifies to clear all WAC sessions.
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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear the authentication sessions.

Example

This example shows how to remove authentication sessions on Ethernet port 1/0/1.

```
Switch# clear authentication sessions interface eth1/0/1
Switch#
```

69-9 authentication username mac-format

This command is used to configure the MAC address format that will be used for authenticating as the username via the RADIUS server. Use the **no** form of this command to return to the default setting.

authentication username mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}

no authentication username mac-format

Parameters

lowercase	Specifies that when using the lowercase format, the RADIUS authentication username will be formatted as: aa-bb-cc-dd-ee-ff.
uppercase	Specifies that when using uppercase format, the RADIUS authentication 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 dot.

The default authentication MAC address delimiter number is 2.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the formatting of usernames used for RADIUS authentication or for IGMP security based on the MAC address.

Example

This example shows how to format the username based on the MAC address.

```
Switch# configure terminal
```

```
Switch(config)# authentication username mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

69-10 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 the command to reset to default setting.

authentication max users *NUMBER*

no authentication max users

Parameters

NUMBER	Specifies to set the maximum authenticated users' number. The range is from 1 to 4096.

Default

None.

Command Mode

Global Configuration Mode.

Interface Configuration Mode.

Command Default Level

Level: 12.

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.

The maximum users being limited include 802.1X, MAC-based Access Control, and WAC 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)#
```

69-11 authentication mac-move deny

This command is used to enable MAC move on the switch. Use the **no** form of this command to return to the default setting.

authentication mac-move deny

no authentication mac-move deny

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command control whether to allow authenticated hosts to do roaming across different switch ports. This command only controls whether a host which is authenticated at a port set to **multi-auth** mode is allowed to move to another port.

If a station is allowed to move, there are two situations. It may either need to be re-authenticated or directly moved to the new port without re-authentication based on the following rule. If the new port has the same authentication configuration as the original port, then re-authentication is not needed. The host will inherit the same authorization attributes with new port. The authenticated host can do roaming from port 1 to port 2, and inherit the authorization attributes without re-authentication. If the new port has the different authentication configuration as the original port, then re-authentication is needed. The authenticated host on port 1 can move and re-authenticated by port 2. If the new port has no authentication method enabled, then the station is directly moved to the new port. The session with the original port is removed. The authenticated host on port 1 can be moved to port 2.

If MAC move is disabled and an authenticated host moves to another port, then this is treated as a violation error.

Example

This example shows how to enable MAC move on a switch.

```
Switch# configure terminal
Switch(config)# authentication mac-move deny
Switch(config)#
```

69-12 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.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for authentication, the authorized attributes (for example VLAN, 802.1p default priority, bandwidth, and ACL) assigned by the RADIUS server will be accepted if the authorization status is enabled. Bandwidth and ACL are assigned on a per-port basis. If in the **multi-auth** mode, VLAN and 802.1p are assigned on a per-host basis. Otherwise, Bandwidth and ACL are assigned on a per-port basis.

Example

This example shows how to disable the authorization status.

```
Switch# configure terminal
Switch(config)# no authorization disable
Switch(config)#
```

69-13 show authentication sessions

This command is used to display authentication information.

show authentication sessions [mac | wac | dot1x | interface *INTERFACE-ID* **[, | -] [mac | wac | dot1x] | mac-address** *MAC-ADDRESS***]**

Parameters

mac	Specifies to display all MAC sessions.
wac	Specifies to display all WAC sessions.
dot1x	Specifies to display all dot1x sessions.
interface *INTERFACE-ID*	(Optional) Specifies a port to display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
mac-address *MAC-ADDRESS*	(Optional) Specifies to display a specific user.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command without parameters to display the sessions associated with all ports.

Example

This example shows how to display sessions on Ethernet port 1/0/1.

```
Switch# show authentication sessions interface eth1/0/1

Interface: eth1/0/1
MAC Address: 00-16-76-35-1A-38
Authentication VLAN: 1
Authentication State: Success
Accounting Session ID: 0000000000CB
Authentication Username: wac
Client IP Address: 10.90.90.9
Aging Time: 3590 sec
Method   State
  WEB-based Access Control: Success, Selected

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.
Accounting Session ID	The accounting session ID that used to do accounting after authenticated.
Authentication Username	It indicates the user name of host. It's not available while the host is selected by MAC-Auth.
Client IP Address	It indicates the address of the client associates. It's only available while the host is selected by Web-Auth or JWAC.
Assigned VID	Effectively assigned VLAN ID that was authorized after the host passed authentication.
Assigned Priority	Effectively assigned priority that was authorized after the host passed authentication.
Assigned Ingress Bandwidth	Effectively assigned ingress that was authorized after the host passed authentication.
Assigned Egress Bandwidth	Effectively assigned egress that was authorized after the host passed

	authentication.
Method	The Authentication method, such as 802.1X, MAC-Auth, Web-Auth, JWAC, etc…
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.
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.
Idle Time	**Idle Time**: Indicates the leftover time of an authenticated session that will be terminated if the session sustains no activity for the configured period of time. It is only available for WEB sessions.
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.

70. Network Load Balancing (NLB) Commands

70-1 nlb unicast-fdb

This command is used to add a unicast MAC entry to the NLB unicast address table. Use the **no** form of the command to remove a unicast entry from the NLB unicast address table or remove interfaces from an NLB entry.

nlb unicast-fdb *MAC-ADDR* **interface** *INTERFACE-ID* **[, | -]**

no nlb unicast-fdb *MAC-ADDR* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

MAC-ADDR	Specifies the MAC address of the entry. The address must be a unicast address. If a received packet contains a destination MAC address that matches the specified MAC address, it will be forwarded to the specified interface.
interface *INTERFACE-ID*	Specifies the interface to which the matched packets will be forwarded. Only physical ports are valid interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces are allowed before and after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an NLB unicast MAC entry. The Network Load Balancing (NLB) function is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all the servers, but will only be processed by one of them. The server can work in two different modes:

- **Unicast mode:** The client uses a unicast MAC address as the destination MAC address to reach the server.
- **Multicast mode:** The client uses a multicast MAC address as the destination MAC address to reach the server.

This destination MAC address is called the shared MAC address. However, the server uses its own MAC address (rather than the shared MAC address) as the source MAC address in the reply packet. In other words, a NLB unicast address usually is not the source MAC address of a packet.

When the received packet contains the destination MAC address matches the configured unicast MAC address, it will be forwarded to those configured ports, regardless of the VLAN membership configuration.

Administrators cannot configure a static address of the MAC address table as a NLB address. However, if a MAC address is created as a NLB MAC address entry, the same MAC address can be still dynamically

learnt in the Layer 2 MAC address table. In this situation, the NLB has higher priority; the dynamically learnt FDB entry won't take effect.

Example

This example shows how to add an NLB unicast address 00-F3-22-0A-12-F4 to the MAC address table. The candidate forwarding interfaces are eth2/0/1 to eth2/0/5.

```
Switch# configure terminal
Switch(config)# nlb unicast-fdb 00-F3-22-0A-12-F4 interface eth2/0/1-5
Switch(config)#
```

70-2 nlb multicast-fdb

This command is used to add an entry to the NLB multicast address table. Use the **no** form of the command to remove an NLB entry from the NLB multicast address table or remove interfaces from a multicast NLB entry.

nlb multicast-fdb *MAC-ADDR* **vlan** *VLAN-ID* **interface** *INTERFACE-ID* **[, | -]**

no nlb multicast-fdb *MAC-ADDR* **vlan** *VLAN-ID* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

MAC-ADDR	Specifies the MAC address of the entry. The address must be a multicast address. If a received packet contains a destination address that matches the specified MAC address it will be forwarded to the specified interfaces.
vlan *VLAN-ID*	Specifies the VLAN ID of the entry. The range is 1 to 4094.
interface *INTERFACE-ID*	Specifies the interface to which the matched packets will be forwarded to. Only physical ports are valid interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces are allowed before and after the comma.
-	(Optional)Specifies a range of interfaces. No spaces are allowed before and after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an NLB multicast MAC address entry. This destination MAC address is called the shared MAC address. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet. In other words, an NLB unicast address usually is not the source MAC address of a packet.

The NLB multicast and Layer 2 multicast FDB are mutually exclusive. The IPv6 multicast mapped MAC addresses (33:33:xx:xx:xx:xx) and IEEE reserved MAC addresses (01:80:c2:00:00:xx) are forbidden to

set as the NLB multicast MAC address. NLB entry 01:00:5E:xx:xx:xx (IPv4 multicast mapped MAC address) has higher priority.

Example

This example shows how to add a multicast address 01-F3-22-0A-12-F4 received on VLAN 1 candidate forwarding ports eth2/0/1 to eth2/0/5 to the NLB multicast address table.

```
Switch# configure terminal
Switch(config)# nlb multicast-fdb 01-F3-22-0A-12-F4 vlan 1 interface eth2/0/1-5
Switch(config)#
```

70-3 show nlb fdb

This command is used to display NLB configured entries.

show nlb fdb

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display NLB configured entries, including unicast and multicast entries.

Example

This example shows how to display NLB configured entries, including unicast and multicast entries.

```
Switch# show nlb fdb

MAC Address         VLAN ID        Interface
----------------- ----------  ---------------------------------
00-F3-22-0A-12-F4 -           eth 1/0/1-1/0/5
01-F3-22-0A-12-F4 1           eth 1/0/6-1/0/9

Total Entries : 2

Switch#
```

71. Open Shortest Path First Version 2 (OSPFv2) Commands

71-1 area default-cost

This command is used to specify the cost associated with the type-3 default route that will be automatically injected into the stub area and the not-so-stubby area. Use the **no** command to revert to the default setting.

area *AREA-ID* **default-cost** *COST*

no area *AREA-ID* **default-cost**

Parameters

AREA-ID	Specifies the ID of the area. The ID can be specified as either a decimal value or an IP address.
COST	Specifies the cost for the default route. The acceptable value is a 24-bit number from 0 to 65535.

Default

By default, this value is 1.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command on the Area Border Router (ABR) that is attached to the stub-area or NSSA area to specify the cost associated with the type-3 default route generated to the area.

Example

This example shows how to assign a default cost of 20 to the stub area 10.0.0.0.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 10.0.0.0 default-cost 20
Switch(config-router)#
```

71-2 area nssa

This command is used to assign an area as an NSSA area. Use the **no** command to remove the NSSA related settings associated with the area.

area *AREA-ID* **nssa [no-summary]**

no area *AREA-ID* **nssa [no-summary]**

Parameters

AREA-ID	Specifies the ID of the area to be assigned as an NSSA area.
no-summary	(Optional) Specifies that this function only takes effect when the router is an ABR.

Default

No NSSA area is defined.

If **no-summary** is not specified, the summary route will be advertised to the NSSA area.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command **no area** *AREA-ID* **nssa** removes all NSSA related settings associated with the area. The area remains as an NSSA area.

There are no external routes in an OSPF stub area, so routes cannot be redistributed from another protocol into a stub area.

An NSSA allows external routes to be advertised to the area in the type-7 LSA. These routes are then leaked into other areas. Although, the external routes from other areas still do not enter the NSSA.

Use the **area nssa** command to simplify administration if connecting a central site using OSPF to a remote site that is using a different routing protocol. Extend OSPF to cover the remote connection by defining the area between the central router and the remote router as a NSSA.

For ASBR NSSA redistribution, external routes will only be redistributed to the NSSA area when redistribution is configured for the associated OSPF process.

The external routes from other areas within the same AS will not be injected to the NSSA area.

If there are multiple default routes generated into the NSSA area, the following priority will be followed: intra-route > inter-route > external route.

Example

This example shows how to configure the NSSA area.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 nssa
Switch(config-router)#
```

71-3 area range

This command is used to summarize OSPF routes at an area border router. Use the **no** command to remove the defined summarization of routes.

area *AREA-ID* **range** *PREFIX/PREFIX-LENGTH* **[advertise | not-advertise]**

no area *AREA-ID* **range [***PREFIX/PREFIX-LENGTH***]**

Parameters

AREA-ID	Specifies the area from which the routes will be summarized.
PREFIX/PREFIX-LENGTH	Specifies the prefix and length of the prefix of the summary route.
advertise	(Optional) Specifies to advertise a Type-3 summary LSA for the specified range of addresses.
not-advertise	(Optional) Specifies to suppress the advertising of Type-3 summary LSAs. Component routes are still hidden behind it.

Default

By default, this option is disabled.

If **advertise** or **not-advertise** is not specified, the default option is **advertise**.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be applied to the same area multiple times. Use this command on the ABR to summarize the intra-area routes. This command can be used to specify the summarized route for area 0 or for the non-zero area. Multiple area range commands can be configured. Thus, OSPF can summarize addresses for multiple sets of address ranges.

Example

This example shows how to configure one summary route to be advertised by the ABR to other areas for all subnets on network 192.168.0.0.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 range 192.168.0.0 255.255.0.0
Switch(config-router)#
```

71-4 area stub

This command is used to specify an area as a stub area. Use the **no** command to remove the stub related settings associated with the area.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Parameters

AREA-ID	Specifies the ID of the area to be assigned as a stub area.
no-summary	(Optional) Specifies that the stub area is a total stub area.

Default

By default, an area is a normal area.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command **no area** *AREA-ID* **stub** removes all stub related settings associated with the area. The area remains as a stub area. Use this command on all routers in the stub area.

Use the **no-summary** keyword to specify the area as a total stubby area. Routers in the area do not require to know the inter-area routes except a type-3 default route.

Example

This example shows how to configure area 3 as stub area.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 stub
Switch(config-router)#
```

71-5 area virtual-link

This command is used to configure a link between a non-backbone area that is physically separated from the backbone area. Use the **no** command to remove a virtual link or reset the specific parameter to the default value.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[authentication [message-digest | null]] [dead-interval** *SECONDS***] [hello-interval** *SECONDS***] [[authentication-key** *PASSWORD***] | [message-digest-key** *KEY-ID* **md5** *KEY***]]**

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[dead-interval | hello-interval | authentication | authentication-key | message-digest-key** *KEY-ID***]**

Parameters

AREA-ID	Specifies the identifier of the area to establish the virtual link. It can be specified as either a decimal value or as an IPv4 address.
ROUTER-ID	Specifies the router ID of the virtual link neighbor.
authentication	(Optional) Specifies the authentication type. If the authentication type is not specified for the virtual link, the password authentication type for the area will be used.
message-digest	(Optional) Specifies that message-digest authentication is used for the virtual link.
null	(Optional) Specifies that no authentication is used.
hello-interval *SECONDS*	(Optional) Specifies the hello packet interval that the router sends on the virtual link. This value must be between 1 and 65535 seconds. If not specified, the default value is 10 seconds.
dead-interval *SECONDS*	(Optional) Specifies the dead interval time that a neighbor is regarded as off-line if no hello packets are received within that time. This value must be between 1 and 65535 seconds. If not specified, the default value is 40 seconds.
authentication-key *PASSWORD*	(Optional) Specifies an up to 8 bytes long password used for password authentication.
message-digest-key *KEY-ID*	(Optional) Specifies an up to 16 bytes long MD key for MD5 message

md5 *KEY*	digest authentication.

Default

No area ID is predefined.

No router ID is predefined.

The default authentication type is NULL.

No authentication-key is predefined.

No message-digest-key is predefined.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If a non-zero area is not physically connected to the zero area, it must be connected to the zero area via a virtual link. The virtual link is a point-to-point link. The router will send the OSPF message to the neighbor router as unicast IP packet.

Example

This example shows how to establish a virtual link with a hello-interval and dead-interval of 5 and 10 seconds respectively.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# area 1 virtual-link 10.10.11.50 dead-interval 10 hello-interval
5
Switch(config-router)#
```

This example shows how to configure the parameters for a virtual link at area 1 and remote ID of 192.168.255.1. The key is defined is a simple password authentication, defined as “yourpass” and the authentication type is set to simple password.

```
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# area 1 virtual-link 192.168.255.1 authentication
Switch(config-router)# area 1 virtual-link 192.168.255.1 authentication-key yourpass
Switch(config-router)#
```

71-6 clear ip ospf

This command is used to restart the IPv4 OSPF process.

clear ip ospf process [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

When an OSPF process is cleared, the OSPF routing database will be cleared and the process is restarted.

Example

This example shows how to clear the OSPF process.

```
Switch# clear ip ospf process
Switch#
```

71-7 default-information originate

This command is used to generate a default external route (type-5 LSA) network 0.0.0.0 to the AS. Use **no** command to disable the generation of the type-5 LSA default route.

default-information originate [always] [metric *METRIC-VALUE***]**

no default-information originate [always] [metric]

Parameters

always	(Optional) Specifies to always generate the default route regardless of existence of a default route in the redistricted routes.
metric *METRIC-VALUE*	(Optional) Specifies the cost associated the generated default route. If not specified, the default metric cost is 1. The valid value is from 1 to 65535.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The **default-information originate** command is used in the ASBR to configure a routing process to advertise a default route (network 0.0.0.0) to the routing domain. If **always** is specified, the default route is generated all the time. If **always** is not specified, the default route will only be generated when the default route exists in the redistributed routes.

Example

This example shows how to advertise the default route regardless of the existence of a default route in the software.

```
Switch# configure terminal
```

```
Switch(config)# router ospf
Switch(config-router)# default-information originate always
Switch(config-router)#
```

71-8 default-metric (OSPF)

This command is used to configure the default metric value for the routing protocol. Use the **no** command to remove the default metric setting.

default-metric *METRIC-VALUE*

no default-metric

Parameters

METRIC-VALUE	Specifies the default metric value for the redistributed routes. The valid value is from 1 to 16777214.

Default

By default, this value is 20.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The **default-metric** command is used in conjunction with the **redistribute router configuration** command to cause the current routing protocol to use the default metric value for the redistributed routes that have no metric specified.

Example

This example shows how to configure router redistributes RIP-derived routes into the OSPF domain and that all redistributed routes are advertised with an OSPF metric of 10.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# default-metric 10
Switch(config-router)# redistribute rip
Switch(config-router)#
```

71-9 distance ospf

This command is used to configure the distance for specific OSPF routes. Use the **no** form of the command to restore to the default setting.

distance ospf {inter-area | intra-area | external-1 | external-2} *DISTANCE*

no distance ospf

Parameters

inter-area	Specifies the distance for OSPF inter-area routes.
intra-area	Specifies the distance for OSPF intra-area routes.
external-1	Specifies the distance for OSPF external type-5 and type-7 routes with a type-1 metric.
external-2	Specifies the distance for OSPF external type-5 and type-7 routes with a type-2 metric.
DISTANCE	Specifies the administrative distance. This value must be between 10 and 255.

Default

By default, the Inter-area distance is 90.

By default, the Intra-area distance is 80.

By default, the External-1 distance is 110.

By default, the External-2 distance is 115.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **distance ospf** command to set the administrative distance for specific OSPF routes. The **distance ospf** command acts as the distance command which determines which routes will be installed in routing information base. If the distance of specific OSPF routes is not configured, the distance follows the value specified by the distance command.

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value is, the lower the rating of trustworthiness is. An administrative distance of 255 means that the routing information source cannot be trusted and should be ignored.

Example

This example shows how to configure the distance of external routes type-1 metric to 50.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# distance ospf external-1 50
Switch(config-router)#
```

71-10 host area

This command is used to configure a stub host entry belonging to a particular area. Use the **no** command to remove the host area configuration.

host *IP-ADDRESS* **area** *AREA-ID* **[cost** *COST***]**

no host *IP-ADDRESS* **area** *AREA-ID*

Parameters

IP-ADDRESS	Specifies the IP address of the host.
AREA-ID	Specifies the identifier of the area that contains the stub host entry.
COST	Specifies cost for the stub host entry. The range is from 0 to 65535.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The router will advertise specific host routes as the router's LSA for a stub link.

Example

This example shows how to configure a stub host 172.16.10.100 at area 1.

```
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# host 172.16.10.100 area 1
Switch(config-router)#
```

71-11 ip ospf authentication

This command is used to define the authentication mode for OSPF. Use the **no** command to disable the authentication.

ip ospf authentication [message-digest]

no ip ospf authentication

Parameters

message-digest	(Optional) Specifies to use the message digest authentication.

Default

By default, no authentication is applied.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When it is specified to use the authentication key but the key is not configured, then NULL key will be used. When it is specified to use message digest but the digest key is not configured, the NULL key (with key ID 0) will be used.

Example

This example shows how to enable message authentication on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)#
```

71-12 ip ospf authentication-key

This command is used to specify an OSPF authentication password for the authentication with the neighboring routers. Use the **no** command to remove an OSPF authentication password.

ip ospf authentication-key *PASSWORD*

no ip ospf authentication-key

Parameters

PASSWORD	Specifies the authentication password of up to 8 bytes. The syntax is general string that does not allow spaces.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command creates a password (key) that is inserted into the OSPF header when the router originates routing protocol packets. Assign a separate password to each network for different interfaces. Routers on the same network must use the same password to be able to exchange OSPF routing data. Configure the routers in the same routing domain with the same password.

Example

This example shows how an authentication key test is created on interface VLAN 1 in area 0. Note that first authentication is enabled for area 0.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf  authentication-key test
Switch(config-if)# ip ospf authentication
Switch(config-if)#
```

71-13 ip ospf cost

This command is used to specify the cost of sending packets on an interface. Use the **no** command to remove the assignment.

ip ospf cost *COST*

no ip ospf cost

Parameters

cost *COST*	Specifies the value of the link-state metric. The range of value is from 1 to 65535.

Default

By default, cost is not configured. The cost is automatically calculated.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The interface cost reflects the overhead for sending the packet across the interface. This cost is advertised as the link cost in the router link advertisement. The cost is inversely proportional to the speed of an interface. The cost can be either manually assigned or be automatically determined.

By default, the cost of an interface is calculated based on reference bandwidth. The cost corresponds that the reference bandwidth is 1. Use the **auto-cost reference-bandwidth** command to set the reference bandwidth. Use the **ip ospf cost** command to manually specify the cost.

Example

This example shows how to configure the interface cost value to 10 on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf cost 10
Switch(config-if)#
```

71-14 ip ospf dead-interval

This command is used to configure the interval during which at least one hello packet form a neighbor must be received before it is declared offline.

ip ospf dead-interval *SECONDS*

no ip ospf dead-interval

Parameters

SECONDS	Specifies the interval in seconds. The range of value is from 1 to 65535. A neighbor is regarded as offline if no packets are received during the interval.

Default

The default interval is 40 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The dead-interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be the same for all routers on a specific network. Specifying a smaller dead interval ensures faster detection of topology changes but might cause more routing instability.

Example

This example shows how to configure the dead interval value to 10 seconds on the VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf dead-interval 10
Switch(config-if)#
```

71-15 ip ospf hello-interval

This command is used to specify the interval between hello packets. To return to the default setting, use the **no** form of this command.

ip ospf hello-interval *SECONDS*

no ip ospf hello-interval

Parameters

SECONDS	Specifies the interval in seconds. This value must be between 1 and 65535 seconds.

Default

By default, this value is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes but generates more routing traffic and might cause routing instability.

Example

This example shows how to configure the hello-interval to 3 seconds on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf hello-interval 3
Switch(config-if)#
```

71-16 ip ospf message-digest-key

This command is used to configure the MD5 digest key for OSPF MD5 authentication. Use the **no** command to remove an MD5 key.

ip ospf message-digest-key *KEY-ID* **md5** *KEY*

no ip ospf message-digest-key *KEY-ID*

Parameters

KEY-ID	Specifies the key identifier. The range is from 1 to 255.
KEY	Specifies the OSPF MD5 message digest key. The syntax is general string that does not allow spaces. This key can be up to 16 characters long.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The authentication for OSPF messages can be either operated in the password mode or MD5 digest mode. This command defines the message digest key used by the MD5 digest mode.

In MD5 digest mode, the OSPF message sender will compute a message digest based on the message digest key for the TX message. The message digest and the key ID will be encoded in the packet. The receiver of the packet will verify the digest in the message against the digest computed based on the locally defined message digest key corresponding to the same key ID.

The same key ID on the neighboring router should be defined with the same key string.

All the neighboring routers on the same interface must use the same key to exchange the OSPF packet with each other. Normally, all neighboring routers on the interface use the same key

With the MD5 digest mode, the user can rollover to a new key without disrupting the current message exchange using the new key. Supposed that a router is currently using an old key to exchange OSPF packets with the neighbor router, as the user configures a new key, the router will start the roll over process by sending duplicated packets for both of the old and the new key. The router will stop sending duplicated packets until it find that all routers on the network have learned the new key. After the rollover process completed, the user should delete the old key to prevent the router from communicating with router using the old key.

Example

This example shows how to configure a new key 10 with the password “yourpass” on the interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf authentication message-digest
Switch(config-if)# ip ospf message-digest-key 10 md5 yourpass
Switch(config-if)#
```

71-17 ip ospf network

This command is used to configure the OSPF network type. To return to the default value, use the **no** form of this command.

ip ospf network {broadcast | point-to-point}

no ip ospf network

Parameters

broadcast	Specifies the network type as broadcast.
point-to-point	Specifies the network type as point-to-point.

Default

The network type is broadcast by default.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to change the OSPF network type of an interface. On a broadcast network, only the designated router and backup designated router become adjacent neighbors of all other routers attached. On point-to-point network, only two routers become adjacent if they can communicate.

Example

This example shows how to configure the OSPF network type to point-to-point on the VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf network point-to-point
Switch(config-if)#
```

71-18 ip ospf priority

This command is used to configure the router priority that is used to determine the designated router for the network. To return to the default value, use the **no** form of this command.

ip ospf priority *PRIORITY*

no ip ospf priority

Parameters

PRIORITY	Specifies the priority of the router on the interface. This value must be between 0 and 255.

Default

By default, this value is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The OSPF router will determine a designated router for the multi-access network.

This command sets the priority used to determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority will be elected the DR. If the routers have the same priority, the router with the higher router ID takes precedence.

Only routers with non-zero router priority values are eligible to become the designated or backup designated router.

Example

This example shows how to configure the OSPF priority value to 3 on the VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip ospf priority 3
Switch(config-if)#
```

71-19 network area

This command is used to enable OSPF routing with the specified area ID on interfaces with IP addresses that match or belong to the specified network address. Use the **no** command to remove the configuration.

network *NETWORK-PREFIX NETWORK-MASK* **area** *AREA-ID*

no network *NETWORK-PREFIX NETWORK-MASK* **area** *AREA-ID*

Parameters

NETWORK-PREFIX NETWORK-MASK	Specifies the subnet prefix and subnet mask of the network.
AREA-ID	Specifies the identifier of the area to be created.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create an OSPF area on the interfaces. The area will be created on an interface if the subnet configured on the interface falls in the range of the network specified by the command. The

interface that has a subnet defined that belongs to the network specified, by this command, will be activated.

Example

This example shows how to define the OSPF area 3 on interfaces with the IP address that starts with the octet value of 10.

```
Switch# configure terminal
Switch(config)# router ospf 1
Switch(config-router)# network 10.0.0.0 255.0.0.0 area 3
Switch(config-router)#
```

71-20 no area

This command is used to remove the settings associated with an area.

no area AREA-ID

Parameters

AREA-ID	Specifies the area ID.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to remove the settings associated with an area. The area reverts to a normal area.

Example

This example shows how to clear all options associated with the area 3 and revert it to normal area.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# no area 3
Switch(config-router)#
```

71-21 passive-interface

This command is used to disable the sending and receiving of the OSPF routing updates on an interface. Use the **no** command to enable the sending and receiving of routing updates.

passive-interface {default | *INTERFACE-ID***}**

no passive-interface {default | *INTERFACE-ID***}**

Parameters

INTERFACE-ID	Specifies the routing interface.
default	(Optional) Specifies the default state of a routing interface when its state is not individually specified.

Default

OSPF routing update packets are sent and received on the interface.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If an interface is passive, the OSPF routing update packets are not sent nor received through the specified interface.

Example

This example shows how to configure the interface VLAN 1 to the passive mode.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# passive-interface vlan1
Switch(config-router)#
```

71-22 redistribute

This command is used to redistribute routes from one routing domain into another routing domain. Use the **no** command to disable redistribution.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***] [metric-type** *TYPE-VALUE***] [route-map** *MAP-NAME***]**

no redistribute *PROTOCOL* **[metric] [metric-type] [route-map]**

Parameters

PROTOCOL	Specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: **bgp**, **connected**, **ospf**, **static**, or **rip**. For routing protocols such as Open Shortest Path First (OSPF), these routes will be redistributed as external to the autonomous system.
metric *METRIC-VALUE*	(Optional) Specifies a metric for the redistributed routes. The valid value is from 0 to 16777214.
metric-type *TYPE-VALUE*	(Optional) Specifies the external link type of the route being redistributed into the OSPF routing domain. It can be one of two values: **1:** Specifies to use the Type-1 external route. **2:** Specifies to use the Type-2 external route. If a metric type is not specified, the switch will adopt a Type-2 external

	route.
route-map *MAP-NAME*	(Optional) Specifies the route map that filters the imported routes from this source routing protocol. If not specified, all routes are redistributed.

Default

By default, route redistribution is disabled.

By default, the metric type is Type-2 for external routes.

By default, the route map is set to redistribute all routes.

Command Mode

Router Configuration Mode.

Command Default Level

Level: ,12 15.

Usage Guideline

External Routes can be redistributed to normal areas as type-5 external routes and redistributed to NSSA stub areas as type-7 external routes by the ASBR.

The external route type can be type-1 or type-2. If the redistributed external route is of type-1, the metric represents the internal metric. If the redistributed external route is of type-2, the metric represents the external metric. An internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

By default, connected and static routes will not be redistributed. Use the **redistribute** or the **default-information router configuration** commands only on the ASBR

BGP and RIP can be redistributed to OSPF.

If a metric is not specified, the metric will be the value set by the **default metric** command. If no value is specified by the default metric, routes redistributed from other protocols will get 20 as the metric value with the following exception. BGP will get 1 as the metric value.

Note that if the redistricted route is a default route, then the metric is determined by **default-information originate** command.

Example

This example shows how BGP routes are redistributed into a OSPF domain.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# redistribute bgp metric 100
Switch(config-router)#
```

71-23 router ospf

This command is used to configure an OSPF routing process. To remove an OSPF routing process, use the **no** form of this command.

router ospf [vrf *VPN-NAME***]**

no router ospf [vrf *VPN-NAME***]**

Parameters

vrf *VPN-NAME*	(Optional) Specifies the name of the VPN routing and forwarding (VRF) instance.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the router configuration mode to configure parameters needed by OSPF.

Example

This example shows how to enable OSPF and enter the OSPF router configuration mode.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)#
```

71-24 router-id

This command is used to specify a router ID for the OSPF process. Use the **no** command to return to the default option.

router-id *ROUTER-ID*

no router-id

Parameters

ROUTER-ID	Specifies the router ID in the IPv4 address format.

Default

An IP address is uniquely chosen as the router ID.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The router ID is a 32-bit number assigned to each router running the OSPF protocol. This number uniquely identifies the router within an Autonomous System. Each router has a unique router ID. If the router is already active when this command is configured, the new router ID will not take effect immediately. It is applied on the next reload or manual restart of the OSPF process.

Example

This example shows how to configure the router ID to 10.10.10.60.

```
Switch# configure terminal
```

```
Switch(config)# router ospf 1
Switch(config-router)# router-id 10.10.10.60
Switch(config-router)#
```

71-25 show ip ospf

This command is used to display general information about the OSPF routing process.

show ip ospf [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display general OSPF protocol information. It provides system wide statistics and per-area statistics for OSPF. The LSDB database overflow limit is the capacity for the LSA table size.

Example

This example shows how to display general OSPF protocol information.

```
Switch#show ip ospf

Operational Router ID 222.200.23.1
  Process uptime is 0DT0H18M54S
  Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
  This router is an ABR, ABR Type is Standard (RFC2328)
  This router is an ASBR (injecting external routing information)
  SPF schedule Hold time between two SPFs 3 secs
  Number of external LSA 2010. Checksum 0x3ef91d0
  Number of LSA originated 261
  Number of LSA received 2131
  Number of current LSA 2184
  LSDB database overflow limit is 49152
  Number of areas attached to this router : 5
    Area 0.0.0.0 (BACKBONE)
        Number of interface in this area is 15 active interface number is 15
        Number of fully adjacent neighbors in this area is 15
        SPF algorithm executed 19 times
        Number of LSA 37
    Area 0.0.0.1
        Number of interface in this area is 1 active interface number is 1
        Number of fully adjacent neighbors in this area is 1
```

```
        SPF algorithm executed 19 times
        Number of LSA 53
    Area 0.0.0.3
        Number of interface in this area is 2 active interface number is 2
        Number of fully adjacent neighbors in this area is 2
        Number of fully adjacent virtual neighbors through this area is 1
        SPF algorithm executed 19 times
        Number of LSA 28
    Area 0.0.0.5
        Number of interface in this area is 1 active interface number is 1
        Number of fully adjacent neighbors in this area is 1
        SPF algorithm executed 19 times
        Number of LSA 27
    Area 0.0.0.7
        Number of interface in this area is 1 active interface number is 1
        Number of fully adjacent neighbors in this area is 2
        SPF algorithm executed 19 times
        Number of LSA 29

Switch#
```

71-26 show ip ospf database

This command is used to display the database summary for OSPF information.

show ip ospf [vrf *VRF-NAME***] database**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the database summary for OSPF information.

Example

This example shows how to display information about the database summary for OSPF information.

```
Switch# show ip ospf database

               Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.47.65.160    10.47.65.160    1765 0x8000000e 0x107f 6
```

```
                Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
47.65.49.111    47.65.49.111    1819 0x80000001 0x33da


                Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
2.1.1.0         10.47.65.160      57 0x80000002 0xe15a 2.1.1.0/24

                ASBR-Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.47.65.160    10.47.65.181    1786 0x80000003 0xb756

                Router Link States (Area 0.0.0.61 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Link count
10.47.65.160    10.47.65.160      77 0x80000004 0x24bb 1

                Summary Link States (Area 0.0.0.61 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route
2.1.1.0         10.47.65.160      57 0x80000002 0xff3e 2.1.1.0/24

                NSSA-external Link States (Area 0.0.0.61 [NSSA])

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
1.0.0.0         10.47.65.160     117 0x80000002 0x80e7 N2 1.0.0.0/24      0

                AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route              Tag
1.0.0.0         10.47.65.160     107 0x80000002 0x15e5 E2 1.0.0.0/24      0

Total Entries: 8

Switch#
```

71-27 show ip ospf database adv-router

This command is used to display all of the LSAs generated by the advertising router.

show ip ospf [vrf *VRF-NAME*] **database adv-router** *ROUTER-ID*

Parameters

ROUTER-ID	Specifies the advertising router.

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all of the LSAs generated by the advertising router.

Example

This example shows how to display all of the LSAs generated by the advertising router.

```
Switch# show ip ospf database router adv-router 10.64.84.200

                Router Link States (Area 0.0.0.0)

  LS age: 498
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 : ASBR
  LS Type: router-LSA
  Link State ID: 10.64.84.200
  Advertising Router: 10.64.84.200
  LS Seq Number: 800037c8
  Checksum: 0xd851
  Length: 96
  Number of Links: 2
    Link connected to: Stub Network
     (Link ID) Network/subnet number: 126.10.62.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metric: 1
    Link connected to: Stub Network
     (Link ID) Network/subnet number: 126.10.61.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metric: 1

Total Entries: 1

Switch#
```

71-28 show ip ospf database asbr-summary

This command is used to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

show ip ospf [vrf *VRF-NAME***] database asbr-summary [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

Example

This example shows how to display information about the Autonomous System Boundary Router (ASBR) summary LSAs.

```
Switch# show ip ospf database asbr-summary

               ASBR-Summary Link States (Area 0.0.0.0)

  LS age: 893
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 10.47.65.160 (AS Boundary Router address)
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000003
  Checksum: 0xb756
  Length: 28
  Network Mask: /0
        TOS: 0  Metric: 1

               ASBR-Summary Link States (Area 0.0.0.1)

  LS age: 927
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: ASBR-summary-LSA
  Link State ID: 10.47.65.183 (AS Boundary Router address)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x53ba
  Length: 28
```

```
  Network Mask: /0
        TOS: 0  Metric: 1

Total Entries: 2

Switch#
```

71-29 show ip ospf database external

This command is used to display information about the external LSAs.

show ip ospf [vrf *VRF-NAME***] database external [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the Autonomous System Boundary Router (ASBR) external LSAs.

Example

This example shows how to display information about the Autonomous System Boundary Router (ASBR) external LSAs.

```
Switch# show ip ospf database external

                AS External Link States

  LS age: 1056
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: AS-external-LSA
  Link State ID: 1.0.0.0 (External Network Number)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x17e4
  Length: 36
```

```
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        Forward Address: 47.65.52.2
        External Route Tag: 0

Total Entries: 1

Switch#
```

71-30 show ip ospf database network

This command is used to display information about the network LSAs.

show ip ospf [vrf *VRF-NAME***] database network [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the network LSAs.

Example

This example shows how to display information about the network LSAs.

```
Switch# show ip ospf database network

                Net Link States (Area 0.0.0.0)

  LS age: 1034
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: network-LSA
  Link State ID: 47.65.49.111 (address of Designated Router)
  Advertising Router: 47.65.49.111
  LS Seq Number: 80000001
```

```
  Checksum: 0x33da
  Length: 32
  Network Mask: /24
        Attached Router: 47.65.49.111
        Attached Router: 10.47.65.160

                Net Link States (Area 0.0.0.1)

  LS age: 1015
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 47.65.51.2 (address of Designated Router)
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000001
  Checksum: 0x9ea1
  Length: 32
  Network Mask: /29
        Attached Router: 10.47.65.181
        Attached Router: 10.47.65.160

Total Entries: 2

Switch#
```

71-31 show ip ospf database nssa-external

This command is used to display information about the NSSA-external LSAs.

show ip ospf [vrf *VRF-NAME*] **database nssa-external [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS*]

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the NSSA-external LSAs.

Example

This example shows how to display information about the NSSA-external LSAs.

```
Switch# show ip ospf database nssa-external

                NSSA-external Link States (Area 0.0.0.61 [NSSA])

  LS age: 1161
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 1.0.0.0 (External Network Number For NSSA)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0x82e6
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 110.201.0.1
        External Route Tag: 0

  LS age: 1097
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-NSSA-LSA
  Link State ID: 47.65.55.0 (External Network Number For NSSA)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0xbb07
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 20
        NSSA: Forward Address: 110.201.0.1
        External Route Tag: 0

Total Entries: 2

Switch#
```

71-32 show ip ospf database self-originate

This command is used to display LSAs generated by the local router.

show ip ospf [vrf *VRF-NAME***] database self-originate**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display LSAs generated by the local router.

Example

This example shows how to display LSAs generated by the local router.

```
Switch# show ip ospf database self-originate

               Router Link States (Area 0.0.0.0)

  LS age: 796
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 : ASBR
  LS Type: router-LSA
  Link State ID: 10.64.84.203
  Advertising Router: 10.64.84.203
  LS Seq Number: 800000f1
  Checksum: 0x57c1
  Length: 84
  Number of Links: 5
    Link connected to: a Transit Network
      (Link ID) Designated Router address: 172.0.12.81
      (Link Data) Router Interface address: 172.0.12.82
       Number of TOS metrics: 0
       TOS 0 Metric: 1
    Link connected to: a Transit Network
      (Link ID) Designated Router address: 172.0.14.100
      (Link Data) Router Interface address: 172.0.14.101
       Number of TOS metrics: 0
       TOS 0 Metric: 1
    Link connected to: a Transit Network
      (Link ID) Designated Router address: 172.0.15.2
      (Link Data) Router Interface address: 172.0.15.1
       Number of TOS metrics: 0
       TOS 0 Metric: 1
    Link connected to: a Transit Network
      (Link ID) Designated Router address: 192.0.21.3
      (Link Data) Router Interface address: 192.0.21.2
       Number of TOS metrics: 0
       TOS 0 Metric: 1
    Link connected to: a Transit Network
      (Link ID) Designated Router address: 192.0.22.3
      (Link Data) Router Interface address: 192.0.22.2
       Number of TOS metrics: 0
       TOS 0 Metric: 1
```

```
Total Entries: 1

Switch#
```

71-33 show ip ospf database router

This command is used to display information about the router LSAs.

show ip ospf [vrf *VRF-NAME***] database router [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the router LSAs.

Example

This example shows how to display information about the router LSAs.

```
Switch# show ip ospf database router

                Router Link States (Area 0.0.0.0)

  LS age: 1056
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.47.65.160
  Advertising Router: 10.47.65.160
  LS Seq Number: 8000000e
  Checksum: 0x107f
  Length: 96
  Number of Links: 6
    Link connected to: a Transit Network
     (Link ID) Designated Router address: 47.65.49.111
```

```
     (Link Data) Router Interface address: 47.65.49.1
      Number of TOS metrics: 0
      TOS 0 Metric: 1
    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.181
     (Link Data) Router Interface address: 47.65.51.1
      Number of TOS metrics: 0
      TOS 0 Metric: 1
    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.182
     (Link Data) Router Interface address: 47.65.52.1
      Number of TOS metrics: 0
      TOS 0 Metric: 1
    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.183
     (Link Data) Router Interface address: 47.65.53.1
      Number of TOS metrics: 0
      TOS 0 Metric: 1
    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.184
     (Link Data) Router Interface address: 47.65.54.1
      Number of TOS metrics: 0
      TOS 0 Metric: 1
    Link connected to: Stub Network
     (Link ID) Network/subnet number: 47.65.49.112
     (Link Data) Network Mask: 255.255.255.255
      Number of TOS metrics: 0
      TOS 0 Metric: 0

  LS age: 1063
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.47.65.181
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000006
  Checksum: 0xb55d
  Length: 48
  Number of Links: 2
    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.160
     (Link Data) Router Interface address: 47.65.51.2
      Number of TOS metrics: 0
      TOS 0 Metric: 1
    Link connected to: a Virtual Link
     (Link ID) Neighboring Router ID: 10.47.65.184
     (Link Data) Router Interface address: 47.65.84.2
      Number of TOS metrics: 0
      TOS 0 Metric: 10

Total Entries: 2

Switch#
```

71-34 show ip ospf database summary

This command is used to display information about the summary LSAs.

show ip ospf [vrf *VRF-NAME***] database summary [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the summary LSAs.

Example

This example shows how to display information about the summary LSAs.

```
Switch# show ip ospf database summary

                Summary Link States (Area 0.0.0.0)

  LS age: 1225
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 2.1.1.0 (summary Network Number)
  Advertising Router: 10.47.65.160
  LS Seq Number: 80000001
  Checksum: 0xe359
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 1

  LS age: 1225
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: summary-LSA
  Link State ID: 2.1.2.0 (summary Network Number)
  Advertising Router: 10.47.65.160
```

```
  LS Seq Number: 80000001
  Checksum: 0xd863
  Length: 28
  Network Mask: /24
        TOS: 0  Metric: 1

 Total Entries: 2

 Switch#
```

71-35 show ip ospf database stub

This command is used to display information about the LSAs in the stub and NSSA areas.

show ip ospf [vrf *VRF-NAME***] database stub [***LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.
LINK-STATE-ID	Specifies the link state ID (as an IP address).
self-originate	Specifies the self-originated link states.
adv-router	Specifies to display all the LSAs of the specified router.
IP-ADDRESS	Specifies the advertise router IP address

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the LSAs in the stub and NSSA areas.

Example

This example shows how to display information about the LSAs in the stub and NSSA areas.

```
Switch# show ip ospf database stub

Router Link States (Area 1.1.1.1)

LS age: 1063
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x3 : ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.47.65.181
  Advertising Router: 10.47.65.181
  LS Seq Number: 80000006
```

```
 Checksum: 0xb55d
 Length: 48
 Number of Links: 2
   Link connected to: a Virtual Link
    (Link ID) Neighboring Router ID: 10.47.65.160
    (Link Data) Router Interface address: 47.65.51.2
     Number of TOS metrics: 0
     TOS 0 Metric: 1
   Link connected to: a Virtual Link
    (Link ID) Neighboring Router ID: 10.47.65.184
    (Link Data) Router Interface address: 47.65.84.2
     Number of TOS metrics: 0
     TOS 0 Metric: 10

             Net Link States (Area 1.1.1.1)

 LS age: 1034
 Options: 0x0 (*|-|-|-|-|-|-|-)
 LS Type: network-LSA
 Link State ID: 47.65.49.111 (address of Designated Router)
 Advertising Router: 47.65.49.111
 LS Seq Number: 80000001
 Checksum: 0x33da
 Length: 32
 Network Mask: /24
       Attached Router: 47.65.49.111
       Attached Router: 10.47.65.160

               Summary Link States (Area 1.1.1.1)

 LS age: 1225
 Options: 0x2 (*|-|-|-|-|-|E|-)
 LS Type: summary-LSA
 Link State ID: 2.1.1.0 (summary Network Number)
 Advertising Router: 10.47.65.160
 LS Seq Number: 80000001
 Checksum: 0xe359
 Length: 28
 Network Mask: /24
       TOS: 0  Metric: 1

Total Entries: 3

Switch#
```

71-36 show ip ospf interface

This command is used to display interface information for OSPF.

show ip ospf interface [*INTERFACE-ID***] [vrf** *VRF-NAME***]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID to display.
vrf *VRF-NAME*	(Optional) Specifies to display the interfaces in the VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display interface information for OSPF. If the no interface type or number is specified, OSPF information of all interfaces will be displayed.

Example

This example shows how to display interface information for OSPF.

```
Switch#show ip ospf interface

vlan10 is up, line protocol is up
  Internet Address: 1.0.0.1/8, Area 0.0.0.0
  Router ID 222.200.23.1, Network Type POINT_TO_POINT, Cost: 1
  Transmit Dealy is 1 sec, State PTP, Priority 1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: simple text
  Authentication Key Configuration
    Authentication type: simple text
      Authentication-key: 123

vlan20 is up, line protocol is up
  Internet Address: 2.0.0.1/8, Area 0.0.0.1
  Router ID 222.200.23.1, Network Type BROADCAST, Cost: 1
  Transmit Dealy is 1 sec, State BDR, Priority 1
  Designated Router (ID) 222.200.23.2, Interface Address 2.0.0.2
  Backup Designated Router (ID) 222.200.23.1, Interface Address 2.0.0.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: md5
  Authentication Key Configuration
    Authentication type: md5
      Message-digest-key 1

Total Entries : 2

Switch#
```

71-37 show ip ospf neighbor

This command is used to display information of OSPF neighbors.

show ip ospf neighbor [interface *INTERFACE-ID* **| neighbor** *NEIGHBOR-ID***] [detail] [vrf** *VRF-NAME***]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID to display.
NEIGHBOR-ID	(Optional) Specifies the Neighbor ID.
detail	(Optional) Specifies to display detailed information of neighbors.
vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information of OSPF neighbors. If no interface type or number is specified, OSPF neighbor information of all interfaces will be displayed.

Example

This example shows how to display information of OSPF neighbors.

```
Switch# show ip ospf neighbor

 Neighbor ID     Pri   State           Dead Time   Address         Interface
-------------------------------------------------------------------------------
110.2.2.2         1   Full/DR         00:00:38    10.10.9.2       vlan1
15.15.15.15       1   2-Way/DROther   00:00:38    10.22.8.100     vlan1
110.1.1.1         1   Exchange/Backup 00:00:39    10.90.90.90     vlan1
32.44.67.200      1   Full/DR         00:00:39    21.44.67.200    vlan2

Total Entries: 4
Switch#

Switch#show ip ospf neighbor detail
Neighbor 110.2.2.2, interface address 10.10.9.2
    In the area 0.0.0.0 via interface vlan1
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 10.10.9.2, BDR is 10.90.90.90
    Options is 0x02 (*|-|-|-|-|-|E|-)
    Dead timer due in 00:00:40
    Neighbor is up for 00:00:30
    Crypt Sequence Number is 0

 Neighbor 15.15.15.15, interface address 10.22.8.100
    In the area 0.0.0.0 via interface vlan1
    Neighbor priority is 1, State is 2-Way, 2 state changes
    DR is 10.10.9.2, BDR is 10.90.90.90
```

```
    Options is 0x02 (*|-|-|-|-|-|E|-)
    Dead timer due in 00:00:32
    Neighbor is up for 00:00:28
    Crypt Sequence Number is 0

 Neighbor 110.1.1.1, interface address 10.90.90.90
    In the area 0.0.0.0 via interface vlan1
    Neighbor priority is 1, State is Exchange, 4 state changes
    DR is 10.10.9.2, BDR is 10.90.90.90
    Options is 0x02 (*|-|-|-|-|-|E|-)
    Dead timer due in 00:00:35
    Neighbor is up for 00:00:27
    Crypt Sequence Number is 0

 Neighbor 32.44.67.200, interface address 21.44.67.200
    In the area 0.0.0.1 via interface vlan2
    Neighbor priority is 1, State is Full, 6 state changes
    DR is 21.44.67.200, BDR is 21.44.67.100
    Options is 0x02 (*|-|-|-|-|-|E|-)
    Dead timer due in 00:00:35
    Neighbor is up for 00:00:26
    Crypt Sequence Number is 0

Total Entries: 4
Switch#

Switch# show ip ospf neighbor interface  vlan1
Neighbor ID     Pri   State           Dead Time   Address         Interface
---------------------------------------------------------------------------
110.2.2.2         1   Full/DR         00:00:38    10.10.9.2       vlan1
15.15.15.15       1   2-Way/DROther   00:00:37    10.22.8.100     vlan1
110.1.1.1         1   Exchange/Backup 00:00:38    10.90.90.90     vlan1

Total Entries: 3

Switch#
```

71-38 show ip ospf virtual-links

This command is used to display virtual link information.

show ip ospf virtual-links [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the IPv4 OSPF VRF process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display virtual link information.

Example

This example shows how to display virtual link information.

```
Switch#show ip ospf virtual-links

Virtual Link to router 10.90.90.90 is up
  Transit area 0.0.0.3 via interface vlan40
  Local address 4.0.0.1
  Remote address 4.0.0.2
  Transmit Delay is 1 sec, State Point-To-Point
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Adjacency state Full
  Current Authentication Type: md5
  Authentication Key Configuration
    Authentication type: md5
      message-digest-key 1

Total Entries : 1

Switch#
```

71-39 debug ip ospf

This command is used to turn on the OSPF debug function. Use the **no** form of this command to turn off the OSPF debug function.

debug ip ospf

no debug ip ospf

Parameters

None.

Default

By default the OSPF debug function is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF debug function while the global debug function has been turned on before.

Example

This example shows how to turn on the OSPF debug function.

```
Switch# debug ip ospf
Switch#
```

71-40 debug ip ospf neighbor

This command is used to turn on the OSPF neighbor state debug switch. Use the **no** form of the command to turn off the OSPF neighbor state debug switch.

debug ip ospf neighbor

no debug ip ospf neighbor

Parameters

None.

Default

By default the OSPF neighbor state debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF neighbor state debug switch. When the neighbor state changes or some events happen to change the neighbor state, debug information will printed if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF neighbor state debug switch.

```
Switch# debug ip ospf neighbor
Switch#

NBR 2.2.2.2 state change from LOADING to FULL tic 100
NBR 3.3.3.3 state change from FULL to DOWN tic 100
```

71-41 debug ip ospf interface

This command is used to turn on the OSPF interface state debug switch. Use the **no** form of the command to turn off the OSPF interface state debug switch.

debug ip ospf interface

no debug ip ospf interface

Parameters

None.

Default

By default the OSPF interface state debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF interface state debug switch. When the OSPF interface state changes or some events happen to change the interface state, debug information will print. When DR selection happens, debug information will also print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF interface state debug switch.

```
Switch# debug ip ospf interface
Switch#

intf 10.1.1.1 up tic 10
intf 100.1.1.1 down tic 20
OSPF: Select DR: 2.2.2.2
OSPF: Select BDR: 1.1.1.1
```

71-42 debug ip ospf lsa-originating

This command is used to turn on the OSPF interface state debug switch. Use the **no** form of the command to turn off the OSPF interface state debug switch.

debug ip ospf lsa-originating

no debug ip ospf lsa-originating

Parameters

None.

Default

By default the OSPF interface state debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF LSA originating debug switch. When the LSA is originated, debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF LSA originating debug switch.

```
Switch# debug ip ospf lsa-originating
Switch#

Build Router LSA id 100.1.1.2 for area 0.0.0.0 seq 80000001 tic 10
```

71-43 debug ip ospf lsa-flooding

This command is used to turn on the OSPF LSA flooding debug switch. Use the **no** form of the command to turn off the OSPF LSA flooding debug switch.

debug ip ospf lsa-flooding

no debug ip ospf lsa-flooding

Parameters

None.

Default

By default the OSPF LSA flooding debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF LSA flooding debug switch. When the LSA is received, added into local database, or flooded to neighboring router, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF LSA flooding debug switch.

```
Switch# debug ip ospf lsa-flooding
Switch#

Received LSA type 1 id 2.2.2.2 from nbr 2.2.2.2 in area 0.0.0.0 seq 80000001 csum fe3a
tic 15
Flood LSAs in area 0.0.0.0 tic 15
```

71-44 debug ip ospf packet-receiving

This command is used to turn on the OSPF packet receiving debug switch. Use the **no** form of the command to turn off the OSPF packet receiving debug switch.

debug ip ospf packet-receiving

no debug ip ospf packet-receiving

Parameters

None.

Default

By default the OSPF packet receiving debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF packet receiving debug switch. When one OSPF protocol packet is received, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF packet receiving debug switch.

```
Switch# debug ip ospf packet-receiving
Switch#

Received a Hello packet from addr 10.1.1.2 at interface System tic 100
Received a Hello packet from addr 100.1.1.2 at interface ip100 tic 102
```

71-45 debug ip ospf packet-transmitting

This command is used to turn on the OSPF packet transmitting debug switch. Use the **no** form of the command to turn off the OSPF packet receiving debug switch.

debug ip ospf packet-transmitting

no debug ip ospf packet-transmitting

Parameters

None.

Default

By default the OSPF packet transmitting debug switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF packet transmitting debug switch. When one OSPF protocol packet is sent out, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF packet transmitting debug switch.

```
Switch# debug ip ospf packet-transmitting
Switch#
```

```
Send out a Hello on interface 10.1.1.1 dst 255.0.0.5 tic 200
Send out a Hello on interface 100.1.1.1 dst 255.0.0.5 tic 220
```

71-46 debug ip ospf spf

This command is used to turn on the OSPF SPF calculation debug switch. Use the **no** form of the command to turn off the OSPF SPF calculation debug switch.

debug ip ospf spf

no debug ip ospf spf

Parameters

None.

Default

By default the OSPF SPF calculation switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF SPF calculation debug switch. When one SFP calculation is processing, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF SPF calculation debug switch.

```
Switch# debug ip ospf spf
Switch#

Running SPF-intra for area 0.0.0.0 tic 300
SPF-intra calculation completed tic 310
```

71-47 debug ip ospf timer

This command is used to turn on the OSPF timer debug switch. Use the **no** form of the command to turn off the OSPF timer debug switch.

debug ip ospf timer

no debug ip ospf timer

Parameters

None.

Default

By default the OSPF timer switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF timer debug switch. When the event related to the OSPF timer happens, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF timer debug switch.

```
Switch# debug ip ospf timer
Switch#

Start Hello timer at interface System tic 20
Wait timer expired at interface System tic 100
```

71-48 debug ip ospf virtual-link

This command is used to turn on the OSPF virtual link debug switch. Use the **no** form of the command to turn off the OSPF virtual link debug switch.

debug ip ospf virtual-link

no debug ip ospf virtual-link

Parameters

None.

Default

By default the OSPF virtual link switch is turned off if the OSPF debug function is turned on.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF virtual link debug switch. When the event related to the OSPF virtual link happens, the debug information will print.

Example

This example shows how to turn on the OSPF virtual link debug switch.

```
Switch# debug ip ospf virtual-link
Switch#

Virtual link up transit area 1.1.1.1 vnbr 3.3.3.3 tic 260
```

71-49 debug ip ospf route

This command is used to turn on the OSPF route debug switch. Use the **no** form of the command to turn off the OSPF route debug switch.

debug ip ospf route

no debug ip ospf route

Parameters

None.

Default

By default the OSPF route switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF route debug switch. When one OSPF route is added, updated or deleted, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF route debug switch.

```
Switch# debug ip ospf route
Switch#

Add an OSPF route level 1 dst 172.18.1.1 mask 255.255.255.0  nh cnt 1 cost 10 cost2: 0
tic: 300
```

71-50 debug ip ospf redistribution

This command is used to turn on the OSPF redistribution debug switch. Use the **no** form of the command to turn off the OSPF redistribution debug switch.

debug ip ospf redistribution

no debug ip ospf redistribution

Parameters

None.

Default

By default the OSPF redistribution switch is turned off.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the OSPF redistribution debug switch. When one route of other protocol is redistributed into OSPF or not redistributed into OSPF any more, the debug information will print if the OSPF debug function is turned on.

Example

This example shows how to turn on the OSPF redistribution debug switch.

```
Switch# debug ip ospf redistribution
Switch#

Import AS external route from src 5 net 192.1.1.1  mask 255.255.255.0 type 2 cost 50
fwd 10.1.1.100 tic 500
```

71-51 debug ip ospf show counter

This command is used to display OSPF statistic counters.

debug ip ospf show counter [packet | neighbor | spf]

Parameters

packet	Specifies to displays the OSPF packet counter.
neighbor	Specifies to displays the OSPF neighbor counter.
spf	Specifies to displays the OSPF SPF event counter.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to check statistic information about OSPF packet, neighbor and SPF calculations.

Example

This example shows how to displays all OSPF statistic counters.

```
Switch# debug ip ospf show counter

OSPF Debug Statistic Counters
Packet Receiving:
  Total  : 5
  Hello  : 5
  DD     : 0
  LSR    : 0
```

```
  LSU    : 0
  LSAck  : 0
  Drop   : 0
  Auth Fail : 0

Packet Sending:
  Total  : 5
  Hello  : 5
  DD     : 0
  LSR    : 0
  LSU    : 0
  LSAck  : 0

Neighbor State:
  Change : 3
  SeqMismatch : 0

SPF Calculation:
  Intra  : 1
  Inter  : 1
  Extern : 1

Switch#
```

71-52 debug ip ospf clear counter

This command is used to reset OSPF statistic counters.

debug ip ospf clear counter [packet | neighbor | spf]

Parameters

packet	Specifies to reset the OSPF packet counter.
neighbor	Specifies to reset the OSPF neighbor counter.
spf	Specifies to reset the OSPF SPF event counter.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to reset OSPF statistic counters. After the reset, the specified counters will change to 0.

Example

This example shows how to reset all OSPF statistic counters.

```
Switch# debug ip ospf clear counter
Switch#
```

71-53 debug ip ospf show database

This command is used to view detailed information about the OSPF LSDB.

debug ip ospf show database {rt-link | net-link | summary-link | external-link | type7-link}

Parameters

rt-link	Specifies to display detailed information of Router LSAs.
net-link	Specifies to display detailed information of Network LSAs.
summary-link	Specifies to display detailed information of Summary LSAs.
external-link	Specifies to display detailed information of AS external LSAs.
type7-link	Specifies to display detailed information of type-7 LSAs.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to view detailed information about the OSPF LSDB.

Example

This example shows how to displays detailed information about Router LSAs.

```
Switch# debug ip ospf show database rt-link

OSPF Phase2 RT Link:

===========
AREA 0.0.0.0:
 Router LSA:
 Link-State ID: 100.1.1.2
 Advertising Router: 100.1.1.2
 LS Age: 10 Seconds
 Options: 0x2
 .... ...0 = 0 Bit Isn't Set
 .... ..1. = E: ExternalRoutingCapability
 .... .0.. = MC: NOT Multicast Capable
 .... 0... = N/P: NSSA Bit
 ...0 .... = EA: Not Support Rcv And Fwd EA_LSA
 ..0. .... = DC: Not Support Handling Of Demand Circuits
```

```
 .0.. .... = O: O Bit Isn't Set
 0... .... = 7 Bit Isn't Set
 LS Sequence Number: 0x80000001
 Length: 36
 Flags: 0x0
 .... ...0 = B: NO Area Border Router
 .... ..0. = E: NO AS Boundary Router
 .... .0.. = V: NO Virtual Link Endpoint
 Number Of Links: 1
 Type: Stub       ID: 10.1.1.0         Data: 255.255.255.0    Metric: 1
 Internal Field:
 Del_flag: 0x0  I_ref_count: 0  Seq: 0x80000001  Csum: 0x4d28
 Rxtime: 0  Txtime: 0  Orgage: 0
 Current Time: 10

Switch#
```

71-54 debug ip ospf show request-list

This command is used to display current LSA information of the internal OSPF request list.

debug ip ospf show request-list

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to check the information about LSAs that OSPF is requesting to neighbors

Example

This example shows how to display current requested LSAs.

```
Switch# debug ip ospf show request-list

OSPF Request List:

*Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
 LSID: 192.194.134.0  RTID: 90.2.0.1
 LSID: 192.194.135.0  RTID: 90.2.0.1
 LSID: 192.194.136.0  RTID: 90.2.0.1
 LSID: 192.194.137.0  RTID: 90.2.0.1
```

```
 LSID: 192.194.138.0  RTID: 90.2.0.1

Switch#
```

71-55 debug ip ospf show redistribution

This command is used to display the current internal OSPF redistribution list.

debug ip ospf show redistribution

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to check the information about the external routes imported into OSPF.

Example

This example shows how to display the external routes imported into OSPF.

```
Switch# debug ip ospf show redistribution

OSPF Redistribution List:

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

OSPF ASE Table:

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

Switch #
```

71-56 debug ip ospf show summary-list

This command is used to display the current internal OSPF summary list.

debug ip ospf show summary-list

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to check the information about the route to be aggregated.

Example

This example shows how to display route information to be aggregated.

```
Switch# debug ip ospf show summary-list

OSPF Summary List:

Area 0.0.0.0:
Circuit: 1.1.1.1
Neighbor: 90.2.0.1  IP: 1.1.1.2
LSID: 1.1.1.1 RTID: 1.1.1.1

Circuit: 2.2.2.1

Circuit: 10.1.1.6

Switch #
```

72. Open Shortest Path First Version 3 (OSPFv3) Commands

72-1 area default-cost

This command is used to set the summary-default cost of a stub area. To disable this function, use the **no** form of this command.

area *AREA-ID* **default-cost** *COST*

no area *AREA-ID* **default-cost**

Parameters

AREA-ID	Specifies the identifier of the area which routes are to be summarized. It can be specified as an IPv4 address.
COST	Specifies the metric or cost for this summary route, which is used during IPv6 OSPF calculation to determine the shortest paths to the destination. The value can be 0 to 65535.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used only on an ABR attached to a stub area. In all routers and access servers attached to the stub area, the area should be configured as a stub area using the **area stub** command. Use the **area default-cost** command only on an ABR attached to the stub area. The **area default-cost** command provides the metric for the summary default route generated by the ABR into the stub area.

Example

This example shows how to assign a default cost of 10 to stub area 1.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1000
Switch(config-rtr)# area 0.0.0.1 stub
Switch(config-rtr)# area 0.0.0.1 default-cost 10
Switch(config-rtr)#
```

72-2 area range

This command is used to consolidate and summarize routes at an area boundary. To disable this function, use the **no** form of this command.

area *AREA-ID* **range** *IPv6-PREFIXIPREFIX-LENGTH* **[advertise | not-advertise]**

no area *AREA-ID* **range** *IPv6-PREFIXIPREFIX-LENGTH*

Parameters

AREA-ID	Specifies the identifier of the area which routes are to be summarized. It can be specified as an IPv4 address.
IPv6-PREFIX	Specifies the IPv6 prefix.
PREFIX-LENGTH	Specifies the IPv6 prefix length.
advertise	(Optional) Specifies to advertise and generate a Type-3 summary LSA for the specified address range.
not-advertise	(Optional) Specifies to set the status to Do-Not-Advertise for the specified address range. The Type-3 summary LSA is suppressed, and the component networks remain hidden from other networks.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used only with ABRs. It is used to consolidate or summarize routes for an area. The result is that a single summary route is advertised to other areas by the ABR. Routing information is condensed at area boundaries. External to the area, a single route is advertised for each address range.

Example

This example shows how to configure one summary route to be advertised by the ABR to other areas for IPv6 prefix 2001:0DB8:0:1::/64 and for the Router ID 20.0.1.10.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1000
Switch(config-rtr)# router-id 20.0.1.10
Switch(config-rtr)# area 0.0.0.1 range 2001:0DB8:0:1::/64
Switch(config-rtr)#
```

72-3 area stub

This command is used to define an area as a stub area. To disable this function, use the **no** form of this command.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Parameters

AREA-ID	Specifies the identifier of the area which routes are to be summarized. It can be specified as an IPv4 address.

no-summary	(Optional) Specifies to prevent an ABR from sending summary LSAs into the stub area.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command on all routers in the stub area. There are two stub area router configuration commands: the **stub** and **area default-cost** commands. In all routers attached to the stub area, configure the area by using the stub option of the area command. For an ABR attached to the stub area, use the **area default-cost** command.

Use the **no-summary** parameter with this command to define a totally stubby area. Define an area as a totally stubby area, when routers in the area do not require learning about summary LSAs from other areas. The area can be defined as a totally stubby area by configuring the ABR of that area using the **area stub no-summary** command.

Example

This example shows how to configure the router as a stub that advertises connected and summary routes.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1000
Switch(config-rtr)# router-id 20.0.1.10
Switch(config-rtr)# area 1.1.1.1 stub
Switch(config-rtr)#
```

72-4 area virtual-link

This command is used to define an IPv6 OSPF virtual link. To remove a virtual link, use the **no** form of this command.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[hello-interval** *SECONDS***] [dead-interval** *SECONDS***] [transmit-delay** *SECONDS***] [retransmit-interval** *SECONDS***] [instance-id** *INSTANCE-ID***]**

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[dead-interval | hello-interval | transmit-interval | retransmit-interval]**

Parameters

AREA-ID	Specifies the identifier of the area which routes are to be summarized. It can be specified as an IPv4 address.
ROUTER-ID	Specifies the router ID associated with the virtual link neighbor. It can be specified as an IPv4 address.
INSTANCE-ID	(Optional) Specifies the instance identifier.
hello-interval *SECONDS*	(Optional) Specifies the interval in seconds, between the hello packets that the router sends on an interface. The valid setting is 1-65535.

dead-interval *SECONDS*	(Optional) Specifies the interval in seconds, during which no packets are received and after which a neighbor is regarded as off-line. The valid setting is 1-65535.
transmit-delay *SECONDS*	(Optional) Specifies the interval that the router waits before it transmits a packet. The valid setting is 1-65535.
retransmit-interval *SECONDS*	(Optional) Specifies the interval that the router waits before it retransmits a packet. The valid setting is 1-65535.

Default

No IPv6 OSPF virtual link is defined.

hello-interval *SECONDS*: 10 seconds.

dead-interval *SECONDS*: 40 seconds.

transmit-delay *SECONDS*: 1 seconds.

retransmit-interval *SECONDS*: 5 seconds.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

All areas in an IPv6 OSPF autonomous system must be physically connected to the backbone area (area 0). In some cases where this physical connection is not possible, you can use a virtual link to connect to the backbone through a non-backbone area. As mentioned above, you can also use virtual links to connect two parts of a partitioned backbone through a non-backbone area. The area through which you configure the virtual link, known as a transit area, must have full routing information. The transit area cannot be a stub area.

In IPv6 OSPF, all non-backbone areas must be connected to a backbone area. If the connection to the backbone is lost, the virtual link repairs the connection. You can configure virtual links between any two backbone routers that have an interface to a common non-backbone area. The protocol treats these two routers joined by a virtual link as if they were connected by an un-numbered point-to-point network. To configure virtual link, include both the transit area ID and the corresponding virtual link neighbor's router ID in the virtual link neighbor.

Configure the hello-interval to be the same for all routers attached to a common network. A short hello interval results in the router detecting topological changes faster but also an increase in the routing traffic.

As with the hello interval, the value of dead-interval must be the same for all routers and access servers attached to a common network.

The retransmit-interval is the expected round-trip delay between any two routers in a network. Set the value to be greater than the expected round-trip delay to avoid needless retransmissions.

The transmit-delay is the time taken to transmit a link state update packet on the interface. Before transmission, the LSUs are incremented by this amount. Set the transmit-delay to be greater than zero. Also, take into account the transmission and propagation delays for the interface.

To configure a virtual link in IPv6 OSPF, you must use a router ID instead of an address. In IPv6 OSPF, the virtual link takes the router ID rather than the IPv6 prefix of the remote router.

Example

This example shows how to establish a virtual link with default values for all optional parameters.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1000
Switch(config-rtr)# area 0.0.0.1 virtual-link 192.168.255.1
Switch(config-rtr)#
```

72-5 auto-cost reference-bandwidth

This command is used to control the reference value IPv6 OSPF uses when calculating metrics for interfaces. To return the reference value to its default, use the **no** form of this command.

auto-cost reference-bandwidth *MBPS*

no auto-cost reference-bandwidth

Parameters

MBPS	Specifies the bandwidth rate in Mbps. The range is from 1 to 4294967. The default is 100.

Default

By default, this value is 100Mbps.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to control the reference value IPv6 OSPF uses when calculating metrics for interfaces.

Example

This example shows how to set the auto-cost reference bandwidth to 1000 Mbps.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1000
Switch(config-rtr)# auto-cost reference-bandwidth 1000
Switch(config-rtr)#
```

72-6 clear ipv6 ospf process

This command is used to restart the OSPF state, based on the OSPF routing process ID.

clear ipv6 ospf [*PROCESS-ID***] process**

Parameters

PROCESS-ID	(Optional) Specifies the internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The OSPF database is cleared, repopulated, and then the SPF algorithm is performed. Use the process ID option to clear only one OSPF process. If the process ID option is not specified, all OSPF processes are cleared.

Example

This example shows how to clear the OSPF database.

```
Switch# clear ipv6 ospf process
Switch#
```

72-7 default-metric

This command is used to set the default metric for IPv6 OSPF. To return the metric to its default value, use the **no** form of this command.

default-metric *METRIC-VALUE*

no default-metric

Parameters

METRIC-VALUE	Specifies the default metric value. This value must be between 1 and 16777214.

Default

The default metric value is 20.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The **default-metric** command is used in conjunction with the **redistribute** router configuration command to cause the current routing protocol to use the same metric value for all redistributed routes. A default metric helps solve the problem of redistributing routes with incompatible metric. Whenever metrics don't convert, using a default metric provides a reasonable substitute and enables the redistribution to proceed.

Example

This example shows how an IPv6 OSPF redistributes routes from the IPv6 RIP. All redistributed routes are advertised with a metric of 10.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1000
Switch(config-rtr)# default-metric 10
```

```
Switch(config-rtr)# redistribute rip
Switch(config-rtr)#
```

72-8 distance ospf

This command is used to configure the distance for specific OSPF routes. Use the **no** form of the command to restore to the default setting.

distance ospf {external | inter-area | intra-area} *DISTANCE*

no distance ospf

Parameters

external	Specifies the distance for OSPF external routes.
inter-area	Specifies the distance for OSPF inter-area routes.
intra-area	Specifies the distance for OSPF intra-area routes.
DISTANCE	Specifies the distance value of specific OSPF routes in the range 1 to 254.

Default

By default, the distance value is 110 for all OSPF routes.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **distance ospf** command to set the administrative distance for specific OSPF routes. The **distance ospf** command acts as the distance command which determines which routes will be installed in routing table.

Numerically, an administrative distance is an integer from 0 to 255. In general, the higher the value is, the lower the rating of trustworthiness is. The administrative distance of 255, means that the routing information source cannot be trusted and should be ignored.

Example

This example shows how to configure the distance of external routes to 50.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1
Switch(config-rtr)# distance ospf external 50
Switch(config-rtr)#
```

72-9 ipv6 ospf area

This command is used to configure an area of an OSPF process on an interface. To disable OSPF routing for the interfaces defined, use the **no** form of this command.

ipv6 ospf *PROCESS-ID* **area** *AREA-ID* **[instance** *INSTANCE-ID***]**

no ipv6 ospf *PROCESS-ID* **area** *AREA-ID* **[instance** *INSTANCE-ID***]**

Parameters

AREA-ID	Specifies the identifier of the area. It can be specified as an IPv4 address.
PROCESS-ID	Specifies the process ID. The ID of a process is used internally and should be uniquely locally assigned.
INSTANCE-ID	(Optional) Specifies Instance identifier. The valid setting is from 0 to 255. If not specified, the default is 0.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command configures an area of an OSPF process on an interface. This setting takes effect only when the configured interface is an IPv6 interface. The created area is a normal area initially and can be changed to another type of area by using the **area stub** command.

On the same interface, only one area can be configured for the same OSPF process. The instance ID is a value representing a specific instance. The instance ID must the same as the neighbor router in order to establish the neighbor session.

Example

This example shows how to create an OSPF area on an interface.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ipv6 address 2001:DB8:0:6::/64 eui-64
Switch(config-if)# ipv6 enable
Switch(config-if)# ipv6 ospf 1000 area 0.0.0.0 instance 2
Switch(config-if)#
```

72-10 ipv6 ospf cost

This command is used to explicitly specify the cost of sending a packet on an interface. To reset the interface cost to the default value, use the **no** form of this command.

ipv6 ospf cost *COST*

no ipv6 ospf cost

Parameters

COST	Specifies the unsigned integer value expressed as the link-state

	metric. It can be a value in the range from 1 to 65535.

Default

By default the cost is not configured.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Set the metric manually using the **ipv6 ospf cost** command. Using the **bandwidth** command changes the link cost as long as the **ipv6 ospf cost** command is not used. The link-state metric is advertised as the link cost in the router link advertisement.

Example

This example shows how to set the interface cost value to 65.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 ospf cost 65
Switch(config-if)#
```

72-11 ipv6 ospf dead-interval

This command is used to set the time period for which hello packets must not be seen before neighbors declare the router down. To return to the default time, use the **no** form of this command.

ipv6 ospf dead-interval *SECONDS*

no ipv6 ospf dead-interval

Parameters

SECONDS	Specifies the interval in seconds, during which no packets are received and after which a neighbor is regarded as off-line. The valid setting is 1-65535.

Default

The default interval is 40 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The interval is advertised in router hello packets. This value must be the same for all routers and access servers on a specific network.

Example

This example shows how to set the IPv6 OSPF dead interval to 60 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 ospf dead-interval 60
Switch(config-if)#
```

72-12 ipv6 ospf hello-interval

This command is used to specify the interval between hello packets that the software sends on the interface. To return to the default time, use the **no** form of this command.

ipv6 ospf hello-interval *SECONDS*

no ipv6 ospf hello-interval

Parameters

SECONDS	Specifies the interval in seconds, between the hello packets that the router sends on an interface. The valid setting is 1-65535.

Default

The default interval is 10 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This value is advertised in the hello packets. The shorter the hello interval, the earlier topological changes will be detected, but more routing traffic will ensue. This value must be the same for all routers and access servers on a specific network.

Example

This example shows how to set the interval between hello packets to 15 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 ospf hello-interval 15
Switch(config-if)#
```

72-13 ipv6 ospf priority

This command is used to set the router priority, which helps determine the designated router for this network. To return to the default value, use the **no** form of this command.

ipv6 ospf priority *PRIORITY*

no ipv6 ospf priority

Parameters

PRIORITY	Specifies the number value of the priority of the router. The range is from 0 to 255.

Default

By default, the router priority is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Set the priority to help determine the OSPF Designated Router (DR) for a network. If two routers attempt to become the DR, the router with the higher router priority becomes the DR. If the router priority is the same for two routers, the router with the higher router ID takes precedence.

Only routers with nonzero router priority values are eligible to become the designated or backup designated router. Configure router priority for multi-access networks (not point-to-point) only.

Example

This example shows how to set the router priority value to 4.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 ospf priority 4
Switch(config-if)#
```

72-14 ipv6 ospf retransmit-interval

This command is used to specify the time between LSA retransmissions for adjacencies belonging to the interface. To return to the default value, use the **no** form of this command.

ipv6 ospf retransmit-interval *SECONDS*

no ipv6 ospf retransmit-interval

Parameters

SECONDS	Specifies the interval the router waits before it retransmits a packet. The valid setting is 1-65535.

Default

The default interval is 5 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement during the set time (the retransmit interval value), it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Example

This example shows how to set the retransmit interval value to 6 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 ospf retransmit-interval 6
Switch(config-if)#
```

72-15 ipv6 ospf transmit-delay

This command is used to set the estimated time required to send a link-state update packet on the interface. To return to the default value, use the **no** form of this command.

ipv6 ospf transmit-delay *SECONDS*

no ipv6 ospf transmit-delay

Parameters

SECONDS	Specifies the interval the router waits for before it transmits a packet. The valid setting is 1-65535.

Default

The default interval is 1 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

LSUs must have their ages incremented by the amount specified in the seconds argument before transmission. The value assigned should take into account the transmission and propagation delays for the interface.

If the delay is not added before transmission over a link, the time in which the LSA propagates over the link is not considered. This setting has more significance on very low speed links.

Example

This example shows how to set the transmit delay value to 3 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 ospf transmit-delay 3
Switch(config-if)#
```

72-16 ipv6 router ospf

This command is used to configure an IPv6 OSPF routing process and enter the router configuration mode. To remove an OSPF routing process, use the **no** form of this command.

ipv6 router ospf *PROCESS-ID*

no ipv6 router ospf *PROCESS-ID*

Parameters

PROCESS-ID	Specifies the ID for an IPv6 OSPF routing process. It is locally assigned and should be unique for each IPv6 OSPF routing process on the router. The range of value is from 1 to 65535.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the OSPF for IPv6 router configuration mode. From this mode, you can configure other settings of IPv6 OSPF.

Example

This example shows how to enable the router configuration mode of IPv6 OSPF. The process ID is 1.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1
Switch(config-rtr)#
```

72-17 no area

This command is used to remove the specific area that has been created.

no area *AREA-ID*

Parameters

AREA-ID	Specifies the ID of the area.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command removes the specified OSPF area and its configuration, such as area default-cost, area range, area stub, and area virtual-link.

Example

This example shows how to remove area 0.0.0.3 of OSPF process 1.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1
Switch(config-rtr)# no area 0.0.0.3
Switch(config-rtr)#
```

72-18 passive-interface (IPv6)

This command is used to configure the specified network interface or all interfaces as the passive interface. Use the **no** form of the command to restore it to the default.

passive-interface {default | *INTERFACE-ID***}**

no passive-interface {default | *INTERFACE-ID***}**

Parameters

INTERFACE-ID	Specifies the interface as passive interface.
default	(Optional) Specifies all the interfaces as passive interfaces.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If an interface is passive, the OSPF routing update packets are not sent nor received through the specified interface.

Example

This example shows how to configure all interfaces as passive and activates VLAN 1.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1
Switch(config-rtr)# passive-interface default
Switch(config-rtr)# no passive-interface vlan1
Switch(config-rtr)#
```

72-19 redistribute

This command is used to redistribute routes from other routing domain into IPv6 OSPF routing domain. Use the **no** command to disable redistribution.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***] [metric-type** *TYPE-VALUE***]**

no redistribute *PROTOCOL* **[metric] [metric-type]**

Parameters

PROTOCOL	Specifies the source protocol from which routes are being redistributed. It can be one of the following keywords: **connected**, **static**, or **rip**.
METRIC-VALUE	(Optional) Specifies the metric value. When redistributing other processes to an IPv6 OSPF process. The default metric is 20 when no metric value is specified.
TYPE-VALUE	(Optional) Specifies the external link type associated with the default route advertised into the IPv6 OSPF routing domain. It can be one of two values: **1:** Type-1 external route. **2:** Type-2 external route. If a metric type is not specified, the switch adopts a Type-2 external route. This is only for IPv6 OSPF.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A router receiving a link-state protocol with an internal metric will consider the cost of the route from itself to the redistributing router plus the advertised cost to reach the destination. An external metric only considers the advertised metric to reach the destination.

Whenever you use the redistribute or the default-information router configuration commands to redistribute routes into an IPv6 OSPF routing domain, the router automatically becomes an ASBR. However, an ASBR does not, by default, generate a default route into the IPv6 OSPF routing domain.

When routes are redistributed into IPv6 OSPF from protocols other than IPv6 OSPF, and no metric has been specified with the metric-type keyword and type-value argument, IPv6 OSPF will use 20 as the default metric.

Routes configured with the connected keyword affected by this redistribute command are the routes not specified by the router configuration command.

You cannot use the **default-metric** command to affect the metric used to advertise connected routes.

Example

This example shows how IPv6 OSPF redistributes and any prefixes is learned through IPv6 RIP.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1
Switch(config-rtr)# redistribute rip
Switch(config-rtr)#
```

72-20 router-id (IPv6)

This command is used to specify a router ID for the OSPF process. Use the **no** command to return to the automatic router ID.

router-id *ROUTER-ID*

no router-id

Parameters

ROUTER-ID	Specifies the router ID in the IPv4 address format.

Default

By default, an IP address is uniquely chosen as the router ID.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The router ID is a 32-bit number assigned to each router running OSPF. This number uniquely identifies the router within an Autonomous System. Each router has a unique router ID among IPv6 OSPF processes.

Example

This example shows how to specify a fixed router ID.

```
Switch# configure terminal
Switch(config)# ipv6 router ospf 1
Switch(config-rtr)# router-id 10.1.1.1
Switch(config-rtr)#
```

72-21 show ipv6 ospf

This command is used to display general information about OSPF routing processes.

show ipv6 ospf [*PROCESS-ID***]**

Parameters

PROCESS-ID	(Optional) Specifies the internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The information displayed by the **show ipv6 ospf** command is useful in debugging OSPF routing operations.

Example

This example shows how to display general information about OSPF routing processes.

```
Switch#show ipv6 ospf

Routing Process "OSPFv3 3600" with ID 36.0.0.0
  Process uptime is  0DT1H8M45S
  Conforms to RFC 2740
  This router is an ABR; ABR Type is Standard (OSPFv3).
  This router is an ASBR (injecting external routing information).
  Redistributing External Routes from,
     rip with metric 0 with metric-type 2
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Number of LSA originated 159
  Number of LSA received 299
  Number of areas in this router is 5
    Area 0.0.0.0 (BACKBONE) (active)
        Number of interfaces in this area is 7 active interface number is 7
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 15 times
        Number of LSA 44. Checksum Sum 0x15c2dc
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.1 (active)
        Number of interfaces in this area is 1 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 4 times
        Number of LSA 48. Checksum Sum 0x185c7f
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.3 (active)
        Number of interfaces in this area is 1 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 1
        SPF algorithm executed 5 times
        Number of LSA 25. Checksum Sum 0xf2d7f
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.5 (active)
        Number of interfaces in this area is 1 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 3 times
        Number of LSA 26. Checksum Sum 0xe7047
        Number of Unknown LSA 0
```

```
        Area ranges are
    Area 0.0.0.7 (active)
        Number of interfaces in this area is 1 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 3 times
        Number of LSA 26. Checksum Sum 0xe2066
        Number of Unknown LSA 0
        Area ranges are

Switch#
```

72-22 show ipv6 ospf border-routers

This command is used to display the ABRs and ASBRs for the IPv6 OSPF instance.

show ipv6 ospf [*PROCESS-ID***] border-routers**

Parameters

PROCESS-ID	(Optional) Specifies the internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the ABRs and ASBRs information.

Example

This example shows how to display the ABRs and ASBRs for the IPv6 OSPF instance.

```
Switch# show ipv6 ospf border-routers

OSPFv3 Process 1 internal Routing Table
Codes: i - Intra-area route, I - Inter-area route
i 10.76.37.3 [1] is directly connected, TransitArea 0.0.0.1, ABR, Area 0.0.0.0
i 10.76.37.3 [1] is directly connected, vlan2, ABR, TransitArea 0.0.0.1

Switch#
```

72-23 show ipv6 ospf database

This command is used to display the database summary about OSPF routing processes.

show ipv6 ospf [*PROCESS-ID***] database [external | inter-area prefix | inter-area router | link | network | prefix | router] [adv-router** *ROUTER-ID* **| self-originate] [area** *AREA-ID***]**

Parameters

PROCESS-ID	(Optional) Specifies the process ID. The ID of a process is used internally and should be uniquely locally assigned.
adv-router *ROUTER-ID*	(Optional) Specifies to display all the LSAs of the advertising router. The router ID can be specified as an IPv4 address.
external	(Optional) Specifies to display information only about the external LSAs.
inter-area prefix	(Optional) Specifies to display information only about LSAs based on inter-area prefix LSAs.
inter-area router	(Optional) Specifies to display information only about LSAs based on inter-area router LSAs.
link	(Optional) Specifies to display information about the link LSAs.
network	(Optional) Specifies to display information only about the network LSAs.
prefix	(Optional) Specifies to display information on the intra-area-prefix LSAs.
router	(Optional) Specifies to display information only about the router LSAs.
self-originate	(Optional) Specifies to display only self-originated LSAs (from the local router).
AREA-ID	(Optional) Specifies to display all the LSAs of the specified area. It can be specified as an IPv4 address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

A router's collection of LSA data is stored in a link-state database. The contents of the database, when subjected to the Dijkstra algorithm, result in the creation of the OSPF routing table. Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf database** command to provide more detailed information.

Example

This example shows how to display the database summary about OSPF routing processes.

```
Switch# show ipv6 ospf database

OSPFv3 Router with ID (10.76.37.30) (Process 1)

                Link-LSA (Interface vlan2)

ADV Router      Age  Seq#       CkSum   LinkCnt
```

```
10.76.37.3       512 0x80000001 0xdf6f      1
10.76.37.30      400 0x80000001 0x48fa      1

                Link-LSA (Interface vlan3)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.30      400 0x80000001 0x3210      1

                Router-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.3       354 0x8000000a 0x717d      1
10.76.37.30      357 0x80000003 0x34c8      1
10.76.37.79      439 0x8000000c 0x7be0      0

                Inter-Area-Prefix-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   Prefix
10.76.37.3       503 0x80000002 0x8a9f  3ffe:2::/64
10.76.37.3       503 0x80000002 0xb723  3ffe:2::10/128
10.76.37.3       346 0x80000004 0x8e95  3ffe:4::/64
10.76.37.3       346 0x80000003 0x3d6e  3ffe:4::30/128
10.76.37.30      374 0x80000002 0xd345  3ffe:3::/64
10.76.37.30      374 0x80000002 0xd73f  3ffe:4::/64
10.76.37.30      374 0x80000002 0x7e20  3ffe:4::30/128
10.76.37.30      352 0x80000003 0xa570  3ffe:2::/64
10.76.37.30      352 0x80000003 0x0fad  3ffe:2::10/128

                Inter-Area-Router-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   Dest-RtrID
10.76.37.3       366 0x80000001 0x26dd  10.76.37.30

                Intra-Area-Prefix-LSA (Area 0.0.0.0) (BACKBONE)

ADV Router      Age  Seq#       CkSum   Ref-LsType   Ref-LSID        Prefix
10.76.37.3       348 0x8000000a 0x6a0c  Router-LSA   0.0.0.0         3ffe:1::/64
10.76.37.79      468 0x80000001 0xacdb  Network-LSA  0.0.4.1         1234::/16
10.76.37.79      458 0x80000001 0xf028  Router-LSA   0.0.0.0         1234::/16
10.76.37.79      448 0x80000001 0xe631  Router-LSA   0.0.0.0         1234::/16
10.76.37.79      438 0x80000001 0xd243  Router-LSA   0.0.0.0         1234::/16

                Router-LSA (Area 0.0.0.1)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.3       354 0x80000003 0x3cd1      1
10.76.37.30      357 0x80000005 0x757e      1

                Network-LSA (Area 0.0.0.1)

ADV Router      Age  Seq#       CkSum
10.76.37.3       380 0x80000001 0xe8a7

                Inter-Area-Prefix-LSA (Area 0.0.0.1)
```

```
ADV Router      Age  Seq#       CkSum   Prefix
10.76.37.3       346 0x80000003 0x84a6  3ffe:1::/64
10.76.37.30      395 0x80000002 0xd345  3ffe:3::/64

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

ADV Router   Age  Seq#       CkSum   Ref-LsType   Ref-LSID        Prefix
10.76.37.3   370 0x80000002 0xe744  Router-LSA   0.0.0.0         3ffe:2::10/128
10.76.37.3   374 0x80000001 0xd71c  Network-LSA  0.0.0.2         3ffe:2::/64
10.76.37.30  378 0x80000004 0x379b  Router-LSA   0.0.0.0         3ffe:4::30/128

                Router-LSA (Area 0.0.0.3)

ADV Router      Age  Seq#       CkSum   LinkCnt
10.76.37.30      360 0x80000003 0xbdd5      0

                Inter-Area-Prefix-LSA (Area 0.0.0.3)

ADV Router      Age  Seq#       CkSum   Prefix
10.76.37.30      395 0x80000002 0x920e  3ffe:4::30/128
10.76.37.30      395 0x80000002 0xd73f  3ffe:4::/64
10.76.37.30      352 0x80000003 0xaf67  3ffe:2::/64
10.76.37.30      352 0x80000003 0x19a4  3ffe:2::10/128
10.76.37.30      347 0x80000002 0xcb41  3ffe:1::/64

                Intra-Area-Prefix-LSA (Area 0.0.0.3)

ADV Router      Age  Seq#       CkSum   Ref-LsType   Ref-LSID        Prefix
10.76.37.30      359 0x80000003 0xda73  Router-LSA   0.0.0.0         3ffe:3::/64

Switch#
```

This example shows how to display the router LSAs information.

```
Switch# show ipv6 ospf database router

OSPFv3 Router with ID (10.47.65.180) (Process 1)

                Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1766
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x8000000F
  Checksum: 0x9586
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483809
```

```
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.182
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483810
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.183

  LS age: 1766
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.182
  LS Seq Number: 0x800001C3
  Checksum: 0xAD4F
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483649
      Neighbor Interface ID: 2147483809
      Neighbor Router ID: 10.47.65.180
    Link connected to: a Virtual Link
      Metric: 10
      Interface ID: 2147483650
      Neighbor Interface ID: 2147483650
      Neighbor Router ID: 10.47.65.183

Total Entries: 2

Switch#
```

This example shows how to display the network LSAs information.

```
Switch# show ipv6 ospf database network

OSPFv3 Router with ID (47.65.49.1) (Process 1)

                Network-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 68
  LS Type: Network-LSA
  Link State ID: 0.0.4.49
  Advertising Router: 47.65.49.1
  LS Seq Number: 0x80000003
  Checksum: 0xC9D1
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
    Attached Router: 47.65.49.1
    Attached Router: 47.65.49.111

Total Entries: 1
```

```
Switch#
```

This example shows how to display information about inter-area prefix LSAs.

```
Switch# show ipv6 ospf database inter-area prefix

OSPFv3 Router with ID (10.47.65.180) (Process 1)

                Inter-Area-Prefix-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1056
  LS Type: Inter-Area-Prefix-LSA
  Link State ID: 128.64.0.0
  Advertising Router: 47.65.49.111
  LS Seq Number: 0x800000B5
  Checksum: 0x7F28
  Length: 36
  Metric: 0
  Prefix: c800::/64, Prefix Options: 0

Total Entries: 1

Switch#
```

This example shows how to display information about inter-area router LSAs.

```
Switch# show ipv6 ospf database inter-area router

OSPFv3 Router with ID (10.47.65.180) (Process 1)

                Inter-Area-Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 162
  LS Type: Inter-Area-Router-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0x3889
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
  Metric: 1
  Destination Router ID: 10.47.65.183

  LS age: 162
  LS Type: Inter-Area-Router-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0x1862
  Length: 32
  Options: 0x000013 (-|R|-|-|E|V6)
  Metric: 2
  Destination Router ID: 47.65.151.111
```

```
Total Entries: 2

Switch#
```

This example shows how to display information about external LSAs.

```
Switch# show ipv6 ospf database external

OSPFv3 Router with ID (10.47.65.180) (Process 1)

                AS-external-LSA

  LS age: 279
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.1
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0xBF8B
  Length: 32
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 16000000
  Prefix: 1151::/32, Prefix Options: 0 (-|-|-|-)

  LS age: 279
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0xD96D
  Length: 32
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 16000000
  Prefix: 1154::/32, Prefix Options: 0 (-|-|-|-)


  LS age: 279
  LS Type: AS-External-LSA
  Link State ID: 0.0.0.3
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0xDB69
  Length: 32
  Metric Type: 1 (Comparable directly to link state metric)
  Metric: 16000000
  Prefix: 1155::/32, Prefix Options: 0 (-|-|-|-)

Total Entries: 3

Switch#
```

This example shows how to display information about link LSAs.

```
Switch# show ipv6 ospf database link
```

```
OSPFv3 Router with ID (10.47.65.180) (Process 4765)

                Link-LSA (Interface vlan49)

  LS age: 347
  LS Type: Link-LSA
  Link State ID: 0.0.4.49
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x80000003
  Checksum: 0x62B6
  Length: 64
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: fe80::4b0:ff:fe17:31
  Number of Prefixes: 2
    Prefix: 1149::/32, Prefix Options: 0 (-|-|-|-)
    Prefix: 2049:1::/64, Prefix Options: 0 (-|-|-|-)

Total Entries: 1

Switch#
```

This example shows how to display information about intra-area-prefix LSAs.

```
Switch# show ipv6 ospf database prefix

            OSPFv3 Router with ID (10.47.65.180) (Process 1)

                Intra-Area-Prefix-LSA (Area 0.0.0.1)

  LS age: 326
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x8000000B
  Checksum: 0x9814
  Length: 52
  Referenced LS Type: 0x2001
  Referenced Link State ID: 0.0.0.0
  Referenced Advertising Router: 10.47.65.180
  Number of Prefixes: 1
    Prefix: 1152:0:1::1/128, Prefix Options: 2 (-|-|LA|-)
    Metric: 0

  LS age: 1124
  LS Type: Intra-Area-Prefix-LSA
  Link State ID: 0.0.0.2
  Advertising Router: 10.47.65.182
  LS Seq Number: 0x80000024
  Checksum: 0x1F76
  Length: 44
  Referenced LS Type: 0x2002
  Referenced Link State ID: 0.0.8.107
  Referenced Advertising Router: 10.47.65.182
```

```
  Number of Prefixes: 1    Prefix: 2113:1::/64, Prefix Options: 0 (-|-|-|-)
    Metric: 0

Total Entries: 2

Switch#
```

This example shows how to display all the LSAs of the advertising router 10.47.65.182.

```
Switch# show ipv6 ospf database router adv-router 10.47.65.182

            OSPFv3 Router with ID (10.47.65.180) (Process 4765)

                Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1734
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.182
  LS Seq Number: 0x800001D1
  Checksum: 0x915D
  Length: 56
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483649
      Neighbor Interface ID: 2147483809
      Neighbor Router ID: 10.47.65.180
    Link connected to: a Virtual Link
      Metric: 10
      Interface ID: 2147483650
      Neighbor Interface ID: 2147483650
      Neighbor Router ID: 10.47.65.183

Total Entries: 1

Switch#
```

This example shows how to display information about self-originated LSAs.

```
Switch# show ipv6 ospf database router self-originate

            OSPFv3 Router with ID (10.47.65.180) (Process 4765)
                Router-LSA (Area 0.0.0.0) (BACKBONE)

  LS age: 1753
  LS Type: Router-LSA
  Link State ID: 0.0.0.0
  Advertising Router: 10.47.65.180
  LS Seq Number: 0x8000001D
  Checksum: 0x7994
  Length: 56
```

```
  Flags: 0x03 (-|-|E|B)
  Options: 0x000013 (-|R|-|-|E|V6)
  Number of Links: 2
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483809
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.182
    Link connected to: a Virtual Link
      Metric: 1
      Interface ID: 2147483810
      Neighbor Interface ID: 2147483649
      Neighbor Router ID: 10.47.65.183

Total Entries: 1

Switch#
```

72-24 show ipv6 ospf interface

This command is used to display OSPF-related interface information.

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

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID to display the OSPF information. If no interface ID is specified, the OSPF information on all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf interface** command to provide all interfaces' information.

Example

This example shows how to display OSPF-related interface information.

```
Switch# show ipv6 ospf interface

vlan2 is up, line protocol is up
  Link Local Address: fe80::a01:2ff:fe36:2/64
  Interface ID 1026
  OSPFv3 Process (1), Area 0.0.0.1 (active)
```

```
  MTU 1500, Instance ID 0
    Router ID 10.76.37.30, Network Type BROADCAST, Cost: 1 (default)
    Transmit Delay is 1 sec, State BDR, Priority 1
    Designated Router (ID) 10.76.37.3
      Local Address fe80::219:5bff:fef5:2cc1
    Backup Designated Router (ID) 10.76.37.30
      Local Address fe80::a01:2ff:fe36:2
    Timer intervals configured, Hello 10, Dead 40, Retransmit 5
    Neighbor Count is 1, Adjacent neighbor count is 1
    Hello received 32 sent 28, DD received 4 sent 5
    LS-Req received 1 sent 1, LS-Upd received 10 sent 8
    LS-Ack received 6 sent 5, Discarded 0

Switch#
```

72-25 show ipv6 ospf neighbor

This command is used to display OSPF neighbor information on a per-interface basis.

show ipv6 ospf [*PROCESS-ID***] neighbor [***INTERFACE-ID* **|** *NEIGHBOR-ID***] [detail]**

Parameters

PROCESS-ID	(Optional) Specifies the internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.
INTERFACE-ID	(Optional) Specifies the interface ID to display the neighbor information.
NEIGHBOR-ID	(Optional) Specifies the Neighbor ID. It can be specified as an IPv4 address.
detail	(Optional) Specifies to display all neighbors in detail.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Both of these keywords can be appended to all other keywords used with the **show ipv6 ospf neighbor** command to provide all neighbors' information.

Example

This example shows how to display OSPF neighbor information on a per-interface basis.

```
Switch#show ipv6 ospf neighbor detail

Neighbor 12.0.0.1, Link Local address FE80::201:FF:FE00:0
```

```
    In the area 0.0.0.0 via interface vlan8
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 12.0.0.1 BDR is 36.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)

Neighbor 36.20.0.0, Link Local address FE80::2C0:8FFF:FE04:1128
    In the area 0.0.0.0 via interface vlan10
    Neighbor priority is 1, State is FULL, 6 state changes
    DR is 36.20.0.0 BDR is 36.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)

Neighbor 12.0.0.2, Link Local address FE80::202:FF:FE00:0
    In the area 0.0.0.5 via interface vlan11
    Neighbor priority is 1, State is FULL, 5 state changes
    DR is 12.0.0.2 BDR is 36.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)

Total Entries: 3

Switch#
```

72-26 show ipv6 ospf virtual-links

This command is used to display parameters and the current state of OSPF virtual links.

show ipv6 ospf [*PROCESS-ID***] virtual-links**

Parameters

PROCESS-ID	(Optional) Specifies the internally used identification parameter for an IPv6 OSPF routing process. It is locally assigned and can be any positive integer. A unique value is assigned for each IPv6 OSPF routing process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The information displayed by the **show ipv6 ospf virtual-links** command is useful in debugging OSPF routing operations.

Example

This example shows how to display parameters and the current state of OSPF virtual links.

```
Switch# show ipv6 ospf virtual-links
```

```
Virtual Link to router 10.90.90.90 is up
  Transit area 0.0.0.3 via interface vlan40, instance ID 0
  Local Peer Address FD80::2A10:7BFF:FE7D:D963/128
  Remote Peer Address 4000::A/128
  Transmit Delay is 1 sec, State Point-To-Point,
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Adjacency state Full

Total Entries: 1

Switch#
```

73. Policy-based Routing (PBR) Commands

73-1 ip policy route-map

This command is used to specify a route map as the routing policy on an interface. To disable policy routing on the interface, use the **no** form of this command.

ip policy route-map *MAP-NAME*

no ip policy route-map

Parameters

MAP-NAME	Specifies the name of the route map to be used for the routing policy.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is only available for VLAN interface configuration.

Specify one route map as the routing policy on an interface. The policy will be applied to packets received by the interface.

Use the **match ip-address** command in the route map to define the matching criteria for packets with specific characteristics. If the IP access list is used with the **match ip-address** command, all of the matching criteria in the access list will be checked. The packet that matches that permit statement will be acted on based on the route map. The packet that is denied by the access list will be routed based on the routing table.

Use the following set of commands to define the action to take for policy based routing:

- set ip precedence
- set ip next-hop
- set ip default next-hop

If the **no match ip-address** command is used in the specified route-map or if the IP access list configured for the **match ip-address** command of the route-map doesn't exist or exists but contains no rule, the set commands above won't be executed, so the policy on the interface won't take effect.

Example

This example shows how to set up the routing policy to route the packets that match the IP access list name "pbr-acl" to the next-hop 20.1.1.254.

```
Switch# configure terminal
Switch(config)# route-map pbr-map permit 1
Switch(config-route-map)# match ip address pbr-acl
Switch(config-route-map)# set ip next-hop 20.1.1.254
Switch(config-route-map)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip policy route-map pbr-map
Switch(config-if)#
```

73-2 show ip policy

This command is used to display the route map used for policy-based routing.

show ip policy

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use the command to display the policy-based routing information configured on interfaces.

Example

This example shows how to display policy-based information configured on interfaces.

```
Switch# show ip policy

Interface       Route-map
------------ --------------------
vlan1           pbr-map1
vlan2           pbr-map2
vlan100         pbr-map3

Switch#
```

74. Port Security Commands

74-1 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 separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
vlan *VLAN-ID*	Specifies to delete the auto-learned secured entry learned with the specified VLAN.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command clears 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#
```

74-2 show port-security

This command is used to display the current port security settings.

show port-security [[interface *INTERFACE-ID* **[, | -]] [address] | vlan** *VLAN-ID* **[,|-]]**

Parameters

INTEFACE-ID	Specifies the ID of the interface to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
address	Specifies to display all the secure MAC addresses, including both configured and learned entries.
vlan *VLAN-ID*	(Optional) Specifies to display port security settings for the VLAN.
.	(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 and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the current port security settings.

Example

This example shows how to display the port security settings of interfaces eth1/0/1 to eth1/0/3.

```
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 -

Total Entries: 3

Switch#
```

74-3 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*	Specifies to set the maximum number of secure MAC addresses allowed. If not specified, the default value is 32. The valid range is from 1 to 12288.
protect	Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count.
restrict	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	Specifies to shut down the port if there is a security violation and record the system log.
permanent	Specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries.
delete-on-timeout	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*	Specifies to add a secure MAC address to gain port access rights.
permanent	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*	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.

Command Default Level

Level: 12.

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, MAC (MAC-based Access Control), JWAC, WAC 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 at interface eth1/0/1.

```
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)#
```

74-4 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 the command to reset to the default setting.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**

no switchport port-security aging {time | type}

Parameters

MINUTES	Specifies the aging time for the auto-learned dynamic secured address on this port. Its range is from 1 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.

Command Default Level

Level: 12.

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 for interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security aging 1
Switch(config-if)#
```

This example shows how to configure the port security aging time type for interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport port-security aging type inactivity
Switch(config-if)#
```

74-5 port-security limit

This command is used to configure the maximum secure MAC address number on the system or on the specified VLAN. Use the **no** form of this command to reset to the default setting.

port-security limit {global | vlan *VLAN-ID* **[, | -]}** *VALUE*

no port-security limit {global | vlan *VLAN-ID* **[, | -]}**

Parameters

global	Specifies that this setting will be applied to the system.
vlan *VLAN-ID*	Specifies the VLAN ID that will be used.
VALUE	Specifies the maximum number of port security entries that can be learned on the system or specified VLAN. The range is from 1 to 12288. If the setting is smaller than the number of current learned entries, the command will be rejected.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to set the limit on the port security entry number which can be learned on a system or on VLANs.

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)#
```

75. Power Saving Commands

75-1 dim led

This command is used to disable the port LED function. Use the **no** form of the command to restore the LED function.

dim led

no dim led

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn off the port LED function. Use the **no** form of the command to restore the 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)#
```

75-2 power-saving

This command is used to enable individual power saving functions. Use the **no** form of the command to disable these functions.

power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}

no power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}

Parameters

link-detection	Specifies that power saving will be applied by link status.
length-detection	Specifies that power saving will be applied by cable length detection.
dim-led	Specifies that power saving will be applied by scheduled dimming LEDs.

port-shutdown	Specifies that power saving will be applied by scheduled port shutdown.
hibernation	Specifies that power saving will be applied by scheduled system hibernation.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The user can enable or disable link detection, length 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 length detection is enabled, the device can reduce the power consumption of a port dependent on the detected cable length.

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 Energy-Efficient Ethernet (EEE) is enabled, the device will activate EEE power saving for those EEE enabled ports.

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)#
```

75-3 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 the 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.

Command Default Level

Level: 12.

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 eth1/1/1
Switch(config-if)# power-saving eee
Switch(config-if)#
```

75-4 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 the 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.

Command Default Level

Level: 12.

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's LED 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)#
```

75-5 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 the 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.

Command Default Level

Level: 12.

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)#
```

75-6 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 the 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.

Command Default Level

Level: 12.

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)#
```

75-7 show power-saving

This command is used to display the power saving configuration information.

show power-saving [link-detection] [length-detection] [dim-led] [port-shutdown] [hibernation] [eee]

Parameters

link-detection	(Optional) Specifies to display the link detection state.
length-detection	(Optional) Specifies to display the cable length 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If no optional keywords were 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

Length Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Enabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

76. Priority-based Flow Control (PFC) Commands

76-1 clear priority-flow-control counters

This command is used to clear the Priority-based Flow Control (PFC) counters of the specified interface(s).

clear priority-flow-control counters {all | *INTERFACE-ID* **[, | -]} {rx | tx | both}**

Parameters

all	Specifies to clear PFC counters on all interfaces.
INTERFACE-ID	(Optional) Specifies the interface(s) used.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.
rx	Specifies to clear the counter of received PFC frames.
tx	Specifies to clear the counter of transmitted PFC frames.
both	Specifies to clear the counter of received and transmitted PFC frames.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear the PFC counters of requests and indications on the specified interface(s).

Example

This example shows how to clear the counters of transmitted PFC frames on the interface eth3/0/1.

```
Switch# clear priority-flow-control counters eth3/0/1 tx
Switch#
```

76-2 priority-flow-control willing

This command is used to turn on the DCBX PFC willing feature which indicates that the local port is willing to accept PFC configurations from a remote system.

priority-flow-control willing

no priority-flow-control willing

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Priority-based Flow Control (PFC), which is defined in IEEE 802.1Qbb, extends the basic IEEE 802.3x pause semantics and uses the IEEE 802.1p CoS values in the IEEE 802.1Q VLAN tag to differentiate up to eight CoSs that can be subject to flow control independently.

The following is a procedure to enable PFC on a priority basis.

- Use the **class-map type network-qos global configuration** command to create a type network-QoS class map.
- Use the **match cos class-map configuration** command to specify which priorities to configure.
- Use the **policy map type network-qos** command to create a type network QoS policy map.
- Use the **class type network-qos policy-map configuration** command to specify a type network QoS class map to be associated with a traffic policy.
- Use the **pause policy map type network-qos class configuration** command to enable the PFC pause characteristics on a class referenced in a type network QoS policy map.
- Use the **service-policy interface configuration** command to apply a type network QoS policy map.

If the PFC of all priorities is disabled on an interface, the interface defaults to the IEEE 802.3x flow control setting. When the PFC of any priority is enabled, the interface will pause a CoS on which the PFC is enabled and a pause frame for that CoS is received. Meanwhile, a pause frame will be transmitted if congestion is detected on the PFC enabled CoS.

This command is used to turn on the DCBX PFC willing feature that indicates that the local port is willing to accept PFC configurations from a remote system.

Enable the Switch to transmit LLDP DCBX PFC TLVs to advertise the PFC setting per-CoS and negotiate with the peer to take the PFC willing feature into effect.

Example

This example shows how to turn on the DCBX PFC willing bit on the interface eth1/0/3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# priority-flow-control willing
Switch(config-if)#
```

76-3 show interfaces priority-flow-control

This command is used to display PFC information of an interface.

show interfaces [*INTERFACE-ID* **[, | -]] priority-flow-control**

Parameters

INTERFACE-ID	(Optional) Specifies the interface to display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No spaces before and after the comma.
-	(Optional) Specifies a range of interfaces. No spaces before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the PFC information on the specified interfaces.

Example

This example shows how to display PFC information on the specified interface.

```
Switch#show interfaces priority-flow-control

Interface PFC  Admin PFC On      Oper PFC On       Will- Rx PFC    Tx PFC
Id        Cap. Priorities        Priorities        ing   Frame(s)  Frame(s)
--------------------------------  ----------------  --------------------------
eth 1/0/1  8   0,1,2,3,4,5,6,7 0,1,3,4,5           On    4294967295 4294967295
eth 1/0/2  8   0,1,2,3,4,5,6,7 0,1,2,3,4,5,6,7     Off   4294967295 4294967295
eth 1/0/3  8                                      On    0          0
eth 1/0/4  8                                      Off   0          0
eth 1/0/5  8                                      Off   0          0
eth 1/0/5  8                                      Off   0          0
eth 1/0/7  8                                      Off   0          0
eth 1/0/8  8                                      Off   0          0
eth 1/0/9  8                                      Off   0          0
eth 1/0/10 8                                      Off   0          0
eth 1/0/11 8                                      Off   0          0
eth 1/0/12 8                                      Off   0          0
eth 1/0/13 8                                      Off   0          0
eth 1/0/14 8                                      Off   0          0
eth 1/0/15 8                                      Off   0          0
eth 1/0/16 8                                      Off   0          0
eth 1/0/17 8                                      Off   0          0
eth 1/0/18 8                                      Off   0          0
eth 1/0/19 8                                      Off   0          0
eth 1/0/20 8                                      Off   0          0
eth 1/0/21 8                                      Off   0          0
eth 1/0/22 8                                      Off   0          0
eth 1/0/23 8                                      Off   0          0
eth 1/0/24 8                                      Off   0          0
eth 1/0/25 8                                      Off   0          0
eth 1/0/26 8                                      Off   0          0
eth 1/0/27 8                                      Off   0          0
```

```
eth 1/0/28 8                                        Off   0          0

Switch#
```

Display Parameters

PFC Cap	**PFC Capability:** Specifies the device's limitation of how many traffic classes may simultaneously be supported by PFC.
Oper PFC On Priorities	The CoS list that the operational PFC is on. Empty means there is no CoS on which the operational PFC is on at the interface.

77. Private VLAN Commands

77-1 private-vlan

This command is used to configure a VLAN as a private VLAN. Use the **no** form of this command to remove the private VLAN configuration.

private-vlan {community | isolated | primary}

no private-vlan {community | isolated | primary}

Parameters

community	Specifies the VLAN as a community VLAN in a private VLAN domain. Member ports within a community VLAN can communicate with each other but cannot communicate with member ports of other communities at Layer 2.
isolated	Specifies the VLAN as an isolated VLAN in a private VLAN domain. Member ports of an isolate VLAN cannot communicate with each other and with member ports of the community VLAN at Layer 2.
primary	Specifies the VLAN as a primary VLAN in a private VLAN domain.

Default

None.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A private VLAN domain is defined with one primary VLAN, one isolated VLAN, and multiple community VLANs. Use this command first to specify the role of the private VLAN before they can be referenced in other private VLAN configuration commands.

Example

This example shows how to configure a VLAN as a private VLAN. VLAN 1000, VLAN 1001 and VLAN 1002 are configured as a primary VLAN, an isolated VLAN and a community VLAN respectively.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# exit
Switch(config)# vlan 1001
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# exit
Switch(config)# vlan 1002
Switch(config-vlan)# private-vlan community
Switch(config-vlan)#
```

77-2 private-vlan association

This command is used to associate secondary VLANs with a primary VLAN. Use the **no** form of this command to remove the association of secondary VLANs with the primary VLAN.

private-vlan association {add *SECONDARY-VLAN-ID* **[, | -] | remove** *SECONDARY-VLAN-ID* **[, | -]}**

no private-vlan association

Parameters

add *SECONDARY-VLAN-ID*	Specifies to add the association of the specified secondary VLANs with the primary VLAN. The valid ID range of secondary VLAN is from 2 to 4094.
remove *SECONDARY-VLAN-ID*	Specifies to remove the association of the specified secondary VLANs with the primary VLAN.
,	(Optional) Specifies a series of VLAN, or separate a range of VLAN from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLAN. No space is allowed before and after the hyphen.

Default

None.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only one isolated VLAN can be associated with the primary VLAN. Multiple community VLANs can be associated with the primary VLAN. A secondary VLAN can only be associated with one primary VLAN.

Example

This example shows how to associate secondary VLAN 1001 and secondary VLAN 1002 with the primary VLAN 1000.

```
Switch# configure terminal
Switch(config)# vlan 1000
Switch(config-vlan)# private-vlan association add 1001-1002
Switch(config-vlan)#
```

77-3 private-vlan synchronize

This command is used to synchronize secondary VLANs to have the same mapping MST ID as the primary VLAN.

private-vlan synchronize

Parameters

None.

Default

None.

Command Mode

MST Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The secondary VLANs need to be mapped to the same MST ID as the primary VLAN if private VLAN is configured. If the mapping is not synchronized when the user exits the MST Configuration Mode, a warning message will be displayed. Use the **private-vlan synchronize** command to synchronize the MST ID mapping before exiting the MST Configuration Mode. This command will not be saved in the running configuration.

Example

This example shows how to synchronize the MST mapping before exiting the MST Configuration Mode.

```
Switch# configure terminal
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlans 1-100
Switch(config-mst)# instance 2 vlans 101-200
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

77-4 switchport mode private-vlan

This command is used to specify a port as a private VLAN host port or promiscuous port. Use the **no** command to revert the port to the default setting.

switchport mode private-vlan {host | promiscuous}

Parameters

host	Specifies the port as an isolated port or a community port.
promiscuous	Specifies the port as a promiscuous port.

Default

By default, this option is configured as Hybrid VLAN mode.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

For isolated ports or community ports, use the **switchport mode private-vlan host** command to specify the port mode and use the **switchport private-vlan host-association** command to associate the port with the secondary VLAN and the primary VLAN.

For a promiscuous port, use the **switchport mode private-vlan promiscuous** command to specify the port mode and use the **switchport private-vlan mapping** command to associate the port with a primary VLAN and define the mapping secondary VLAN.

For a trunk port of a primary VLAN, use the **switchport mode trunk** command to specify the port mode and use the **switchport trunk allowed vlan** command to define the associated VLANs.

Example

This example shows how to configure physical ports as private VLAN ports. Here, we specify the interface eth1/0/1 as a private VLAN host port and specify the interface eth1/0/2 as a private VLAN promiscuous port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# exit
Switch(config)# interface eth1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)#
```

77-5 switchport private-vlan host-association

This command is used to associate the private VLAN with an isolated port or a community port. Use the **no** command to remove the association.

switchport private-vlan host-association *PRIMARY-VLAN-ID SECONDARY-VLAN-ID*

no switchport private-vlan host-association

Parameters

PRIMARY-VLAN-ID	Specifies the ID of primary VLAN to be associated. The valid ID range of a primary VLAN is from 2 to 4094.
SECONDARY-VLAN-ID	Specifies the ID of secondary VLAN to be associated. The valid ID range of a secondary VLAN is from 2 to 4094.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The port is an isolated port if the secondary VLAN specified by the command is an isolated VLAN. The port is a community port if the secondary VLAN specified by the command is a community VLAN. The command also set the port as untagged member of both the specified secondary VLAN and the primary VLAN.

Example

This example shows how to associate interface eth1/0/1 with the primary VLAN 1000 and the secondary VLAN 1001.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 1000 1001
Switch(config-if)#
```

77-6 switchport private-vlan mapping

This command is used to associate the private VLAN membership with a promiscuous port. Use the **no** command to remove the association.

switchport private-vlan mapping *PRIMARY-VLAN-ID* **{add** *SECONDARY-VLAN-ID* **[, | -] | remove** *SECONDARY-VLAN-ID* **[, | -]}**

no switchport private-vlan mapping

Parameters

PRIMARY-VLAN-ID	Specifies the primary VLAN to be mapped. The valid ID range of the primary VLAN is from 2 to 4094.
add *SECONDARY-VLAN-ID*	Specifies to add membership of the specified secondary VLAN. The valid ID range of secondary VLAN is from 2 to 4094.
remove *SECONDARY-VLAN-ID*	Specifies to remove membership of the specified secondary VLAN.
,	(Optional) Specifies a series of VLAN, or separate a range of VLAN from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLAN. No space is allowed before and after the hyphen.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command configures the port as an untagged member of the specified primary VLAN and the mapping secondary VLANs.

Example

This example shows how to configure interface eth1/0/2 as a private VLAN promiscuous port and to map it to a primary VLAN 1000 and secondary VLAN 1001 and VLAN 1002.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# switchport mode private-vlan promiscuous
Switch(config-if)# switchport private-vlan mapping 1000 add 1001,1002
Switch(config-if)#
```

77-7 show vlan private-vlan

This command is used to display private VLAN configurations.

show vlan private-vlan

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the listing of the private VLAN contained in the private VLAN domain, association of a secondary VLAN with a primary VLAN, and member port of each private VLAN.

Example

This example shows how to display the private VLAN settings. In this example, there are two private VLAN domains configured.

```
Switch# show vlan private-vlan

Primary VLAN   Secondary VLAN   Type           Interface
------------   --------------   ----------   ----------------------------
1000            1001               isolated      eth3/0/1, eth4/0/1
                1002               community
                1003               community
2000            2001               isolated      eth1/0/1, eth1/0/3
2000            2002               community     eth1/0/1, eth1/0/3
2000            2003               community     eth1/0/4, eth1/0/13, eth1/0/15

Total Entries: 6

Switch#
```

78. Protocol Independent Multicast (PIM) IPv6 Commands

78-1 ipv6 pim

This command is used to enable IPv6 PIM Sparse-Mode on an interface. To disable this function, use the **no** form of this command.

ipv6 pim sparse-mode

no ipv6 pim sparse-mode

Parameters

None.

Default

PIM-SM for IPv6 is disabled on all interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Before the PIM function is enabled on an interface, enable IPv6 multicast routing by issuing the command **ipv6 multicast-routing** in the global configuration mode.

Example

This example shows how to enable the IPv6 PIM-SM on a specified interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 pim sparse-mode
Switch(config-if)#
```

78-2 ipv6 pim bsr border

This command is used to specify that the interface is a PIM domain border. To remove the border setting, use **no** form of this command.

ipv6 pim bsr border

no ipv6 pim bsr border

Parameters

None.

Default

By default, no border is configured.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When an interface is configured as a border, it will prevent bootstrap router (BSR) messages from being sent or received through it.

Example

This example shows how to enable the PIM border on the VLAN 1 interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 pim bsr border
Switch(config-if)#
```

78-3 ipv6 pim bsr candidate bsr

This command is used to configure the router to advertise itself as a candidate bootstrap router (BSR). Use the **no** form of this command to remove this router as a candidate for being a BSR.

ipv6 pim bsr candidate bsr *INTERFACE-ID* **[***HASH-MASK-LENGTH***] [priority** *PRIORITY-VALUE***]**

no ipv6 pim bsr candidate bsr

Parameters

INTERFACE-ID	Specifies the interface whose IPv6 address will be announced as the bootstrap router address.
HASH-MASK-LENGTH	Specifies to configure the hash mask length for RP selection. The range is from 0 to 128. The mask (128 bits maximum) that is to be logically *AND* with the group address before the hash function is executed. All groups with the same seed hash (correspond) to the same RP. Therefore one RP can be derived for multiple groups.
priority *PRIORITY-VALUE*	Specifies to configure the priority for a BSR candidate. The range is from 0 to 255. The BSR with the larger priority is preferred. If the priority values are the same, the router with the larger IPv6 address is the BSR.

Default

By default, the router is not a BSR candidate.

HASH-MASK-LENGTH: 126.

PRIORITY-VALUE: 64.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects PIM-SM operation. This command causes the router to send bootstrap messages to all its PIM neighbors, with the address of the designated interface as the BSR address. A PIM-SM domain must contain a unique BSR (Bootstrap router) which is responsible for collect and advertise the RP information.

Example

This example shows how to configure the IPv6 address of VLAN 1 on the router to be a candidate BSR with hash-mask length of 120 and priority of 192.

```
Switch# configure terminal
Switch(config)# ipv6 pim bsr candidate bsr vlan1 120 priority 192
Switch(config)#
```

78-4 ipv6 pim bsr candidate rp

This command is used to configure the candidate rendezvous point (RP) to send Protocol Independent Multicast (PIM) RP advertisements to the bootstrap router (BSR). Use the **no** form of this command to disable PIM RP advertisements to the BSR.

ipv6 pim bsr candidate rp *INTERFACE-ID* **[group-list** *ACCESS-LIST***] [priority** *PRIORITY-VALUE***] [interval** *SECONDS***]**

no ipv6 pim bsr candidate rp *INTERFACE-ID*

Parameters

INTERFACE-ID	Specifies the interface whose IPv6 address will be advertised as the candidate RP (C-RP).
group-list *ACCESS-LIST*	(Optional) Specifies the name of the IPv6 access list that defines the group prefixes that are advertised in association with the RP address. If no group-list is specified, the switch is a candidate RP for all groups.
priority *PRIORITY-VALUE*	(Optional) Specifies the RP priority value. The range is from 0 to 255. The default value is 192.
interval *SECONDS*	(Optional) Specifies the RP candidate advertisement interval. The range is from 1 to 16383 seconds. The default value is 60 seconds.

Default

By default, the router is not an RP candidate.

Priority: 192.

Interval: 60 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects PIM-SM operation. Only one group access list can be specified for each interface. The latest configuration overrides the previous one. This command can be issued multiple times for different interfaces.

This command causes the router to send a PIMv2 message advertising itself as a candidate RP to the BSR.

Example

This example shows how to configure the router with the interface VLAN 1 to be advertised as the candidate RP with a priority of 10.

```
Switch# configure terminal
Switch(config)# ipv6 pim bsr candidate rp vlan1 priority 10
Switch(config)#
```

78-5 ipv6 pim dr-priority

This command is used to change the Designated Router (DR) priority value inserted into the DR priority option of the PIM Hello messages. Use the **no** form of the command to return to the default priority.

ipv6 pim dr-priority *PRIORITY*

no ipv6 pim dr-priority

Parameters

PRIORITY	Specifies the value of the DR priority in the range of 0 to 4294967295. A larger value means a higher priority.

Default

By default, this value is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only valid for the VLAN interface. This command only takes effective when the interface is PIM-SM mode enabled. When a DR is a candidate for election, the following conditions apply:

- The router with the highest priority value configured on an interface will be elected as the DR. If multiple routers have the same highest priority, then the router with the highest IPv6 address configured on the interface will be elected as the DR.
- If a router does not advertise a priority value in its hello messages, the router is regarded as having the highest priority and will be elected as the DR. If there are multiple routers do not include the DR priority option in their hello messages, then the router with the highest IPv6 address will be elected as the DR.

Example

This example shows how to sets the DR priority of the VLAN 1 interface to 200.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 pim dr-priority 200
Switch(config-if)#
```

78-6 ipv6 pim hello-interval

This command is used to configure the frequency of PIM hello messages. Use the **no** form of this command to return to the default interval.

ipv6 pim hello-interval *SECONDS*

no ipv6 pim hello-interval

Parameters

SECONDS	Specifies the interval, in seconds, between Hello messages. The range is from 1 to 18000.

Default

By default, this value is 30 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only valid for the VLAN interface. A PIM router learns PIM neighbors via the hello message. Routers configured for IP multicast send PIM hello messages to detect PIM routers. For SM, hello messages are also used to determine which router will be elected as the designated router for each LAN segment.

Example

This example shows how to configure the PIM hello interval to 45 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 pim hello-interval 45
Switch(config-if)#
```

78-7 ipv6 pim join-prune-interval

This command is used to configure the frequency of PIM periodic join and prune message. Use the **no** form of this command to return to the default interval.

ipv6 pim join-prune-interval *SECONDS*

no ipv6 pim join-prune-interval

Parameters

SECONDS	Specifies the interval, in seconds, between Join and Prune messages. The range is from 1 to 18000.

Default

By default, this value is 60 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only valid for the VLAN interface. This command only takes effect when the interface is PIM-SM enabled.

When configuring the Join/Prune interval, the user needs to consider the factors, such as configured bandwidth and expected average number of multicast route entries for the attached network or link (for example, the period would be longer for lower-speed links, or for routers in the center of the network that expect to have a larger number of entries).

For SM-mode, the router will periodically send the join message based on this interval. The hold-time in a Join/Prune message is 3.5 times the join-prune-interval. The receiving router will start a timer based on this hold-time, and prune the interface if no join message is received on this interface.

Example

This example shows how to configure the PIM Join/Prune timer to 120 seconds on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 pim join-prune-interval 120
Switch(config-if)#
```

78-8 ipv6 pim passive

This command is used to specify an interface running in the passive mode. Use the **no** form of the command to disable passive mode.

ipv6 pim passive

no ipv6 pim passive

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is IPv6 PIM enabled. When the passive mode is enabled, the interface will neither send PIM messages out nor accept PIM messages from this interface. The router will act as it is the only PIM router on the network. Use this command only when there is only one PIM router on the LAN.

Example

This example shows how to configure VLAN 100 as a PIM passive interface.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ipv6 pim passive
Switch(config-if)#
```

78-9 ipv6 pim register-checksum-wholepkt

This command is used to configure the router to calculate the checksum of register message over the entire PIM message including the data portion. Use the **no** form of this command to revert to the default setting.

ipv6 pim register-checksum-wholepkt

no ipv6 pim register-checksum-wholepkt

Parameters

None.

Default

By default, this option is disabled.

By default, the register checksum methodology is PIM RFC-compliant, excluding the data portion in the Register message.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects PIM-SM operation. If this command is specified, then the setting will be applied to all RP addresses.

Example

This example shows how to enable the register checksum over the whole register message.

```
Switch# configure terminal
Switch(config)# ipv6 pim register-checksum-wholepkt
Switch(config)#
```

78-10 ipv6 pim register-probe

This command is used to configure the register-probe time. Use the **no** form of the command to revert to the default setting.

ipv6 pim register-probe *SECONDS*

no ipv6 pim register-probe

Parameters

SECONDS	Specifies the register probe time value in seconds. The range is from 1 to 127.

Default

By default, this value is 5 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The register-probe time is the time before the Register-Stop Timer (RST) expires when a DR may send a Null-Register to the RP to cause it to resend a Register-Stop message.

Example

This example shows how to configure the register-probe time to 10 seconds.

```
Switch# configure terminal
Switch(config)# ipv6 pim register-probe 10
Switch(config)#
```

78-11 ipv6 pim register-suppresion

This command is used to configure the register-suppression time. Use the **no** form of the command to revert to the default setting.

ipv6 pim register-suppression *SECONDS*

no ipv6 pim register-suppression

Parameters

SECONDS	Specifies the register suppression timeout value in seconds. The range is from 3 to 65535.

Default

By default, this value is 60 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects PIM-SM operation.

When a DR receives the register-stop message, it will start the suppression timer. During the suppression time a DR will stop sending Register-encapsulated data to the RP. This timer should be configured on the designated router. The value of the Register Probe Time must be less than half the value of the Register

Suppression Time to prevent a possible negative value in the setting of the Register-Stop Timer. The minimal value for Register Suppression Time is 3.

Example

This example shows how to configure the register suppression time to 30 seconds.

```
Switch# configure terminal
Switch(config)# ipv6 pim register-suppression 30
Switch(config)#
```

78-12 ipv6 pim rp embedded

This command is used to enable embedded RP support in PIMv6. Use the **no** command to disable embedded RP support.

ipv6 pim rp embedded

no ipv6 pim rp embedded

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is PIM-SM enabled.

Embedded RP defines an address allocation policy in which the address of the RP is encoded in an IPv6 multicast group address. This allows an easy deployment of scalable inter-domain multicast and simplifies the intra-domain multicast configuration as well. IPv6 Multicast group addresses embedded with RP information start with ff70::/12 where the flag value of 7 means embedded RP.

Because embedded RP support is enabled by default, the **no** form of this command is generally used, which turns off embedded RP support. The **ipv6 pim rp embedded** command applies only to the embedded RP group ranges ff7x::/12.

Example

This example shows how to disable embedded RP support in IPv6 PIM-SM.

```
Switch# configure terminal
Switch(config)# no ipv6 pim rp embedded
Switch(config)#
```

78-13 ipv6 pim rp-address

This command is used to configure the address of a PIM RP for a particular group range. Use the **no** form of this command to remove an RP address.

ipv6 pim rp-address *IPV6-ADDRESS* **[***GROUP-ACCESS-LIST***] [override]**

no ipv6 pim rp-address *IPV6-ADDRESS*

Parameters

IPV6-ADDRESS	Specifies the IPv6 address of a router to be a PIM RP.
GROUP-ACCESS-LIST	(Optional) Specifies the name of an access list that defines which multicast groups the RP should be used. If no access list is configured, the RP is used for all groups.
override	(Optional) Specifies that the static RP overrides dynamically learned RP.

Default

No RP addresses are preconfigured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects PIM-SM operation. Use this command to statically define the RP address for multicast groups that are to operate in sparse mode.

Users can use a single RP for more than one group. The conditions specified by the access list determine for which groups the RP can be used. Multiple RP can be defined, each with a single access list. The new setting overrides the old one.

All routers in a domain should have a consistent multicast group to RP mapping. The first hop router that initiates a register message will use the mapping entries to determine the RP for sending the PIM register message destined for a specific group. The last hop router that initiates a join message uses the mapping entries to determine the RP for sending the join and prune message for a specific group. When a router receives a join message, it will check the mapping entries for forwarding of the message. When a RP receives a register message, if the router is not the right RP for the multicast group, a register-stop message will be sent.

If the PIM domain is using embedded-RP, only the RP needs to be statically configured as the RP for the embedded RP ranges. The other routers will discover the RP address from the IPv6 group address. If these routers want to select a static RP instead of the embedded RP, the specific embedded RP group range must be configured in the access list of the static RP.

Example

This example shows how to configures the RP address 3ffe:6000:3000::123 for the group access list “G1”.

```
Switch# configure terminal
Switch(config)# ipv6 access-list G1
Switch(config-ipv6-acl)# permit any ff75::/16
Switch(config-ipv6-acl)# exit
Switch(config)# ipv6 pim rp-address 3ffe:6000:3000::123 G1
Switch(config)#
```

78-14 ipv6 pim spt-threshold

This command is used to configure the PIM Shortest Path Tree (SPT) threshold value for the specified groups. Use the **no** form of this command to restore to the default value.

ipv6 pim spt-threshold {0 | infinity}

no ipv6 pim spt-threshold

Parameters

0	Specifies to establish the source tree right at the arrival of the first packet.
infinity	Specifies to always rely on the shared tree.

Default

By default, this option is configured as **infinity**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Using the **infinity** parameter enables all sources for the specified groups to use the shared tree. Using the **0** parameter to join the SPT immediately after the first packet arrives from a new source.

Example

This example shows how to configure the PIM last-hop router to stay on the shared.

```
Switch# configure terminal
Switch(config)# ipv6 pim spt-threshold infinity
Switch(config)#
```

78-15 ipv6 pim sg-keepalive-time

This command is used to configure the PIM6-SM multicast routing entry keep-alive timer.

ipv6 pim sg-keepalive-time *SECONDS*

no ipv6 pim sg-keepalive-time

Parameters

SECONDS	Specifies the period during which the PIM router will maintain the (S, G) state in the absence of explicit (S, G) local membership or (S, G) join messages received to maintain it. The time range is from 120 to 65535 seconds.

Default

By default, this value is 210 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects IPv6 PIM-SM. This command is used to configure the keep-alive timer, which is the period during which the PIM router will maintain the (S, G) state in the absence of explicit (S, G) local membership or (S, G) join messages received to maintain it.

Example

This example shows how to configure the (S, G) keep-alive time to 300 seconds.

```
Switch# configure terminal
Switch(config)# ipv6 pim sg-keepalive-time 300
Switch(config)#
```

78-16 show ipv6 pim

This command is used to display the PIM global information.

show ipv6 pim sparse-mode

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the global information of PIM.

Example

This example shows how to display PIM global information.

```
Switch# show ipv6 pim sparse-mode

Register checksum wholepkt: Enabled
Register probe time          : 10 seconds
Register suppression time     : 60 seconds
SPT Threshold                    : Infinity
(S,G) keepalive time           : 300 seconds
Embedded RP support            : Enabled
RP Address
  3ffe:6000:3000::123, group-list: G1

RP Candidate
```

```
  vlan100, group-list: rp-cand, interval: 60, priority: 192

BSR Candidate
  vlan100, hash-mask-length: 30, priority: 1

Switch#
```

78-17 show ipv6 pim bsr

This command is used to display bootstrap router (BSR) information.

show ipv6 pim bsr {candidate-rp | election | rp-cache}

Parameters

candidate-rp	Specifies to display the C-RP state on routers that are configured as C-RPs.
election	Specifies to displays the BSR state, BSR election, and bootstrap message (BSM) related timers.
rp-cache	Specifies to display the candidate rendezvous point (C-RP) cache learned from unicast C-RP announcements on the elected BSR.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display details of the BSR election-state machine, C-RP advertisement state machine, and the C-RP cache. Information on the C-RP state machine is displayed only on a router configured as a C-RP.

Example

This example shows how to display BSR election information.

```
Switch# show ipv6 pim bsr election

PIMv2 BSR information
BSR Election Information
This system is the Bootstrap Router (BSR)
BSR Address: 3ffe:6000:3000::123
Uptime: 0DT00H18M50S, BSR Priority: 0, Hash mask length: 126
BS Timer: 0DT00H00M21S

Switch#
```

This example shows how to display information that has been learned from various C-RPs at the BSR. In this example, two candidate RPs have sent advertisements for the FF00::/8 or the default IPv6 multicast range.

```
Switch# show ipv6 pim bsr rp-cache

PIMv2 BSR C-RP Cache
BSR Candidate RP Cache
Group(s) FF00::/8
RP 3ffe:1000:10:5::153
Priority 192
Uptime: 0DT00H08M36S, expires: 0DT00H01M21S
RP 3ffe:2000:10:5::100
Priority 192
Uptime: 0DT00H08M36S, expires: 0DT00H01M21S

Switch#
```

This example shows how to display the candidate RP information that had configured on the router.

```
Switch# show ipv6 pim bsr candidate-rp

PIMv2 C-RP information
Candidate RP: 3ffe:1000:10:5::100(vlan10)
  Priority 192, Holdtime 150
  Advertisement interval 60 seconds
  Next advertisement in 0DT00H00M54S

Switch#
```

Display Parameters

This system is the Bootstrap Router (BSR)	Indicates this router is the BSR and provides information on the parameters associated with it.
BS Timer	On the elected BSR, the BS timer shows the time in which the next BSM will be originated. On all other routers in the domain, the BS timer shows the time at which the elected BSR expires.

78-18 show ipv6 pim group-map

This command is used to display the group to RP mapping information.

show ipv6 pim group-map [*IPV6-GROUP-ADDRIPREFIX-LENGTH***] [info-source {bsr | embedded-rp | static}]**

Parameters

IPV6-GROUP-ADDR/PREFIX-LENGTH	(Optional) Specifies the IPv6 multicast group address range.
info-source	(Optional) Specifies to display all mappings learned from a specific

	source, such as the bootstrap router (BSR) or static configuration.
bsr	Specifies to display ranges learned through the BSR.
embedded-rp	Specifies to display group ranges learned through the embedded rendezvous point (RP).
static	Specifies to display ranges enabled by static configuration.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If this command is issued without any parameters, all group mappings will be displayed. Specify the group address range or learned source to filter the group mappings.

Example

This example shows how to display the RP mapping of group FF04::10.

```
Switch# show ipv6 pim group-map ff04::10/128

FF04::10/128
  RP: 3ffe:10:10:5::153
  Info source: 3ffe:10:10:5::153, via bootstrap

Switch#
```

This example shows how to display the RP mappings learned from a specific source enabled by static configurations.

```
Switch# show ipv6 pim group-map info-source static

FF00::/8
    RP: 2013:1:1:11::1
   Info source:  static

Switch#
```

This example shows how to display the RP mappings learned through the embedded rendezvous point (RP).

```
Switch# show ipv6 pim group-map info-source embedded-rp

FF7E:640:2002:6666::/96
    RP: 2002:6666::6
    Info source: embedded

Switch#
```

78-19 show ipv6 pim interface

This command is used to display the configuration for Protocol Independent Multicast (PIM) on interface(s).

show ipv6 pim interface sparse-mode [*INTERFACE-ID***] [detail]**

Parameters

INTERFACE-ID	(Optional) Specifies an interface for display
detail	(Optional) Specifies to display interface information in detail.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to check if PIM is enabled on an interface, the number of neighbors, and the designated router (DR) on the interface. If no interface is specified, the IPv6 PIM information on for all applicable interfaces will be shown.

Example

This example shows how to display how to display the information of the PIM sparse mode interface.

```
Switch#show ipv6 pim interface sparse-mode

PIM6-SM Interface Table

Interface     Mode    Nbr    DR          Hello     J/P       BSR
                      Count  Priority    Interval  Interval  Border
------------  ------  -----  ----------  --------  --------  --------
vlan1         Sparse  1      1           30        60        enabled
    Address         :fe80::207:e9ff:fe02:81d
    Global Address  :3ffe:192:168:1::53
    DR              :fe80::20e:cff:fe01:facc
vlan2     Sparse 2     1        30       60       disabled
    Address         : fe80::207:e9ff:fe02:21a2
    Global Address  : 3ffe:192:168:10::53
    DR              : this system

Total Entries : 2

Switch#
```

This example shows how to displays the PIM information on the interface VLAN 1 in detail.

```
Switch# show ipv6 pim interface sparse-mode vlan1 detail

Interface                                  : vlan1
```

```
Interface Link-Local Address           : fe80::207:e9ff:fe02:81d
Interface Global Address                : 3ffe:192:168:1::53
Mode                                        : Sparse
Designated Router                        : fe80::20e:cff:fe01:facc
Designated Router Priority             : 1
Designated Router Priority Enabled  : True
Generation ID                               : 164585476
Hello Interval                              : 30 seconds
Triggered Hello Interval                : 5 seconds
Hello Holdtime                              : 105 seconds
Join Prune Interval                       : 60 seconds
Join Prune Holdtime                       : 210 seconds
LAN Delay Enabled                         : True
Propagation Delay                         : 1 seconds
Override Interval                         : 3 seconds
Effective Propagation Delay            : 1 seconds
Effective Override Interval            : 3 seconds
Join Suppression Enabled                : True
Bidirectional Capable                     : False
BSR Domain Border                         : Disabled
PIM Passive Mode                          : Enabled

Switch#
```

Display Parameters

Interface	The Interface ID that is configured to perform PIM Sparse mode.
Mode	The PIM mode of this interface.
Nbr Count	The number of PIM neighbors that have been learnt on the interface.
DR Priority	The DR priority that is configured on the interface.
Hello Interval	The hello interval value that is configured on the interface.
J/P Interval	The Join-Prune interval value that is configured on the interface.
BSR Border	The BSR Border state whether is enabled or disabled.
Address	The Link-Local IPv6 address of the interface.
Global Address	The Global IPv6 address of the interface.
DR	The IPv6 address of the designated router of the interface.
Designated Router Priority Enabled	Evaluates if all routers on this interface are using the DR Priority option.
LAN Delay Enabled	Evaluates if all routers on this interface are using the LAN Prune Delay option.
Propagation Delay	The Propagation Delay value of the interface.
Override Interval	The Override Interval value of the interface.
Effective Propagation Delay	The Effective Propagation Delay on this interface.
Effective Override Interval	The Effective Override Interval on this interface.
Join Suppression Enabled	Displays whether join suppression is enabled on this interface.

78-20 show ipv6 pim mroute

This command is used to display the PIM IPv6 multicast routing table.

show ipv6 pim mroute sparse-mode

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all entries in the IPv6 multicast routing table. The switch populates the multicast routing table by creating source, group (S,G) entries from star, group (*,G) entries. The star (*) refers to all source addresses, the "S" refers to a single source address, and the "G" is the destination multicast group address. In creating (S,G) entries, the software uses the best path to that destination group found in the unicast routing table, through Reverse Path Forwarding (RPF).

Example

This example shows how to display the PIM-SM multicast routing table.

```
Switch# show ipv6 pim mroute sparse-mode

PIM-SM Multicast Routing Table:
JP State- Join Prune State, ET - Expiry Timer, PPT - Prune Pending Timer,
KAT - Keep Alive Timer

Flags: S - Sparse, T - SPT-bit set.

(*, ff13::10) Uptime: 0DT00H04M43S, Flags:S
  RP: 3ffe:6000:1005::36, RPF nbr: FE80::217:55FF:FEC0:16, RPF interface: vlan101
  Upstream interface:
   Join State: Joined, Join Timer: 17 secs
  Downstream Interface List:
   vlan11:
     JP State: Join, ET: 166 secs, PPT: off
     Assert State: No Info, Assert Timer: off
      Assert Winner: ::, Metric: 0, Pref: 0

(3ffe:6000:1005::DD, ff13::10) Uptime: 0DT00H00M05S, Flag:ST
  RPF nbr: FE80::217:55FF:FEC0:16, RPF Interface: vlan101
  Upstream Interface:
   Join State: Joined, Join Timer: 55 secs, KAT: off
  Downstream Interface List:
   vlan11:
     JP State: Join, ET: 205 secs, PPT: off
```

```
    Assert State: No Info, Assert Timer: off
     Assert Winner: ::, Metric: 0, Pref: 0

(3ffe:6000:1005::DD, ff13::10, rpt) Uptime: 0DT00H00M05S, Flags:S
  RP: 3ffe:6000:1005::36, RPF nbr: FE80::217:55FF:FEC0:16, RPF Interface: vlan101
  Upstream Interface:
   Prune State: Not Pruned, Override Timer: off
  Downstream Interface List:
   vlan11:
     Prune State: No Info, ET: off, PPT: off

Total Entries: 3

Switch#
```

Display Parameters

Uptime	The time that entry has been created.
Flags	The entry's Sparse/SPT-bit information.
RP	The Rendezvous Point (RP) of the (*, G) mroute entry.
RPF nbr	The Reserve Path Forwarding (RPF) neighbor address.
RPF interface	The local interface name that connect to the upstream router.
Join State	The upstream Join state whether the local router should join the RP tree for the group or join the shortest-path tree for the source and group represented by this entry.
Join Timer	The time remaining before the local router next sends a periodic Join message.
Downstream Interface List	The downstream interface(s) protocol state information.
vlan11	The interface name of the downstream interface.
JP State	The state resulting from (*, G) or (S, G) Join/Prune messages received on this interface.
PPT	The Prune Pending Timer. The remaining time that allows other router to override the join or prune.
ET	The Expiry Timer. The remaining time before the Join state for the interface expire.
Assert State	The assert state of the interface.
Assert Timer	The Assert Timer. If the interface is an Assert Winner, then this timer is the remaining time before the interface to send a assert message. If the interface is an Assert Loser, then this timer is the remaining time before the Assert State expires.
Assert Winner	When the Assert State is Loser, this field is the IP address of the Assert Winner. Otherwise, it is always "::".
Metric	When the Assert State is Loser, this field is metric of the route to the RP/Source that is advertised by the Assert Winner.
Pref	The Preference. When the Assert State is Loser, this field is metric preference of the route to the RP/Source that advertised by the Assert Winner.

78-21 show ipv6 pim neighbor

This command is used to display PIM neighbor information.

show ipv6 pim neighbor sparse-mode [detail] [*INTERFACE-ID*]

Parameters

detail	(Optional) Specifies to display IPv6 PIM neighbor information in detail.
INTERFACE-ID	(Optional) Specifies the interface of which to display the PIM neighbor information. If the interface ID is not specified, the information on all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to determine which routers on the LAN are configured for PIMv6.

Example

This example shows how to display the sparse-mode neighbor information.

```
Switch# show ipv6 pim neighbor sparse-mode

Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
G - Supports Generation ID
Neighbor-Address Interface Uptime/Expires Ver DR Pri/Mode
--------------------------------------------------------------------------------
fe80::a01:2ff:fe39:1
                 vlan1 0DT00H55M33S/0DT00H01M32S v2 1 /G
fe80::a01:2ff:fe39:2
                 vlan2 0DT00H55M30S/0DT00H01M20S v2 1 /DR,G

Total Entries: 2

Switch#
```

Display Parameters

Neighbor-Address	The IPv6 address of the PIM neighbor (link-local address).
Interface	The neighbor's interface name.
Uptime	The length of time that the router has known about this neighbor.
Expires	The time after which the information about this neighbor expires. If the router does not receive any hello messages in this time, it will discard information about this neighbor.

Ver	Indicates the PIM version used by this neighbor.
DR Pri/Mode	The priority and mode of the designated router (DR). **DR Priority:** uses N to indicate that the neighbor does not support the DR Priority option in the Hello message, otherwise, the DR priority value will be displayed. The meaning of indicating codes for Mode are as follows: **DR:** Indicates that the neighbor is the Designated Router. **B:** The neighbor is capable of PIM in the bidirectional mode. **G:** The neighbor supports a Generation ID, which reduces the re-convergence times after a switchover.

79. Protocol Independent Multicast (PIM) Commands

79-1 ip pim

This command is used to enable PIM on the interface for either Sparse Mode (SM) or Dense Mode (DM) operation. Use the **no** command to disable the PIM function on the interface.

ip pim {sparse-mode | dense-mode | sparse-dense-mode}

no ip pim

Parameters

sparse-mode	Specifies to operate in the SM mode.
dense-mode	Specifies to operate in the DM mode.
sparse-dense-mode	Specifies to operate in the SM-DM mode.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface has an IP address configured.

Specify one of the three modes for an interface, sparse mode, dense mode or sparse-dense mode. To switch the PIM operating mode, use the **no ip pim** command to disable PIM first then set the new mode.

Dense Mode - PIM-DM assumes that when a source starts sending, all downstream routers wants to receive the multicast data stream. Initially multicast data stream are flooded to all downstream routers and the interfaces that have group members. If there are no downstream routers or group members, the router will send prune message to indicate that the multicast data stream is not desired.

Sparse Mode - When multicast traffic is received on a sparse mode interface, the first hop router will encapsulate and send the register message to RP. If the router is not the first hop router, the traffic will be forwarded based on the mroute entry.

A sparse mode interface will only be populated as mroute member interface if receive join message from the downstream router or if group member on a sparse mode interface, PIM join process will be triggered to create the shared tree or the source tree.

Sparse-Dense Mode - When interface is configured as PIM Sparse-Dense mode, a multicast group received by the interface can operate in either sparse mode or dense mode of operation. When the interface receives a multicast traffic, if there is a known RP for the group, then this group will be operate in sparse mode, otherwise this multicast group will be operated in dense mode.

Example

This example shows how to enable the PIM-SM protocol on the specified interface.

```
Switch# configure terminal
Switch(config)# interface vlan1
```

```
Switch(config-if)# ip pim sparse-mode
Switch(config-if)#
```

79-2 ip pim bsr-candidate

This command is used to configure the router to announce itself as the Candidate Bootstrap Router (CBSR). Use the **no** form of this command to disable this router to act as a CBSR.

ip pim bsr-candidate *INTERFACE-ID* **[***HASH-MASK-LENGTH* **[***PRIORITY***]] [interval** *SECONDS***]**

no ip pim bsr-candidate

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be announced as the bootstrap router address.
HASH-MASK-LENGTH	Specifies to configure the hash mask length for RP selection. The range is 0 to 32. If not specified, the default length is 30.
PRIORITY	Specifies to configure the priority for a CBSR. The candidate with the highest priority is preferred. If the priority values are the same, the router with the highest IP address is preferred. The range is from 0 to 255. If not specified, the default priority is 64.
interval	Specifies the interval between originating bootstrap messages. If not specified, the default interval is 60 seconds. The valid range is from 1 to 255.

Default

The router is not a CBSR by default.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is specified by the command that has an IP address configured and is PIM-SM enabled.

This command causes the router to send bootstrap messages to announce the IP address of the designated interface as the CBSR address. The hash mask is used by all routers within a domain, to map a group to one of the Rendezvous Points (RP) from the matching set of group-range-to-RP maps (this set all have the same longest mask length and same highest priority). The algorithm takes as an input the group address and the addresses of the candidate RPs from the maps, and gives as an output one RP address to be used.

Example

This example shows how to configure the IP address of the router on VLAN 1 to be a CBSR with a hash-mask length of 20, priority of 192, and interval of 120 seconds.

```
Switch# configure terminal
Switch(config)# ip pim bsr-candidate vlan1 20 192 interval 120
Switch(config)#
```

79-3 ip pim dr-priority

This command is used to configure the Designated Router (DR) priority value. Use the **no** command to restore the default value.

ip pim dr-priority *PRIORITY*

no ip pim dr-priority

Parameters

PRIORITY	Specifies the DR priority value in the range of 0 to 4294967295. A larger value represents the higher priority.

Default

By default, this value is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is PIM-SM enabled.

In the DM mode, the DR priority option will not be carried in the Hello message. The router with the highest priority value will be the DR. If multiple routers are with the same priority status, the router with the highest IP address will be the DR. If there is a router that does not support the DR priority in its Hello message on the LAN, all routers on the LAN will ignore DR priority and only use IP address to elect DR.

Example

This example shows how to configure the DR priority of the VLAN 1 interface to 200.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim dr-priority 200
Switch(config-if)#
```

79-4 ip pim jp-timer

This command is used to configure the Join/Prune interval value. Use the **no** form of the command to restore the default setting.

ip pim jp-timer *SECONDS*

no ip pim jp-timer

Parameters

SECONDS	Specifies the interval between Join/Prune messages. The range is from 1 to 18000.

Default

By default, this value is 60 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is PIM-SM enabled.

When configuring the Join/Prune interval, consider the factors, such as the configured bandwidth and expected average number of multicast route entries for the attached network or link. For the SM-mode, routers will periodically send join messages based on this interval. The hold-time in a Join/Prune message is 3.5 times the join-prune-interval. The receiving router will start a timer based on this hold-time, and prune the interface if no join message was received on this interface.

Example

This example shows how to configure the PIM Join/Prune timer to 120 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim jp-timer 120
Switch(config-if)#
```

79-5 ip pim passive

This command is used to specify an interface running in the passive mode. Use the **no** form of the command to disable the passive mode.

ip pim passive

no ip pim passive

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is PIM enabled.

When the passive mode is enabled, the interface will neither send PIM messages out nor accept PIM messages from this interface. The router will act as if it is the only PIM router on the network.

Use this command only when there is only one PIM router on the LAN.

Example

This example shows how to configure VLAN 100 as a PIM passive interface.

```
Switch# configure terminal
Switch(config)# interface vlan 100
Switch(config-if)# ip pim passive
Switch(config-if)#
```

79-6 ip pim query-interval

This command is used to configure the frequency of the PIM hello message. Use the **no** form of the command to revert to the default setting.

ip pim query-interval *SECONDS*

no ip pim query-interval

Parameters

SECONDS	Specifies the interval at which the hello message is sent.

Default

By default, this value is 30 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is PIM enabled.

A PIMv2 router learns PIM neighbors via the PIM hello message. This command configures the frequency of the hello message. Routers configured for IP multicasting send PIM hello messages to detect PIM routers. For SM, hello messages also determine the router to act as the designated router for each LAN segment. The configured query interval is also used as the value for hold time. By configuring a smaller period for the interval, the unresponsive neighbor can be discovered faster and thus the failover and recovery will become more efficient.

Example

This example shows how to configure the PIM hello interval to 45 seconds.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# ip pim query-interval 45
Switch(config-if)#
```

79-7 ip pim register-checksum-wholepkt

This command is used to enable the calculating of the register checksum value over the whole packet. Use the **no** form of this command to disable calculating the register checksum over the whole packet.

ip pim register-checksum-wholepkt rp-address-list *ACCESS-LIST-NAME*

no ip pim register-checksum-wholepkt

Parameters

ACCESS-LIST-NAME	Specifies the name of the IP access list which specifies a list of RP addresses. This is the address in the source address field of the access list entry.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If this setting is disabled, the checksum for the registered packets is calculated only over the header. This command can be only specified once. The later applied command will override the previous setting.

Example

This example shows how to enable the register checksum over the whole packet when sending to RP of 10.1.1.1.

```
Switch# configure terminal
Switch(config)# ip access-list rp_filter
Switch(config-ip-acl)# permit host 10.1.1.1
Switch(config-ip-acl)# exit
Switch(config)# ip pim register-checksum-wholepkt rp-address-list rp_filter
Switch(config)#
```

79-8 ip pim register-probe

This command is used to configure the register probe time. Use the **no** form of the command to revert to the default setting.

ip pim register-probe *SECONDS*

no ip pim register-probe

Parameters

SECONDS	Specifies the register probe time value in seconds. The range is from 1 to 127.

Default

By default, this value is 5 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The register probe time is the time before the Register Stop Timer (RST) expires when a DR may send a Null-Register to the RP to cause it to resend a Register-Stop message.

Example

This example shows how to configure the register probe time to 7 seconds.

```
Switch# configure terminal
Switch(config)# ip pim register-probe 7
Switch(config)#
```

79-9 ip pim register-suppression

This command is used to configure the register suppression time. Use the **no** form of the command to revert to the default setting.

ip pim register-suppression *SECONDS*

no ip pim register-suppression

Parameters

SECONDS	Specifies the register suppression timeout value in seconds. The range is from 3 to 65535.

Default

By default, this value is 60 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When a DR receives the register stop message, it will start the suppression timer. During the suppression period, a DR stops sending the register message to the RP.

Use this command on the first hop router. The value of the register probe time must be less than half the value of the register suppression time to prevent a possible negative value in the setting of the register stop timer. The minimal value for the register suppression time is 3.

Example

This example shows how to configure the register suppression time to 30 seconds.

```
Switch# configure terminal
Switch(config)# ip pim register-suppression 30
Switch(config)#
```

79-10 ip pim rp-address

This command is used to statically configure the RP address for multicast groups. To remove an RP address, use the **no** form of this command.

ip pim rp-address *IP-ADDRESS* **[group-list** *ACCESS-LIST-NAME***]**

no ip pim rp-address *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IP address of the RP.
group-list *ACCESS-LIST-NAME*	Specifies a standard access list that contains multiple groups. If no group list is specified, the RP will be mapped to all multicast groups.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to specify the static multicast groups to RP mapping. In a multicast domain, the static multicast group to RP mapping can be used together with BSR. All routers in a domain should have a consistent multicast group to RP mapping. The first hop router that initiates a register message will use the mapping entries to determine the RP for sending the PIM register message destined for a specific group. The last hop router that initiates a join message uses the mapping entries to determine the RP for sending the join and prune message for a specific group. When a router receives a join message, it will check the mapping entries for forwarding of the message. When a RP receives a register message, if the router is not the right RP for the multicast group, a register-stop message will be sent.

Multiple RPs can be defined, each with a single access list.

Example

This example shows how to configure the PIM RP address to 10.90.90.90 for multicast group 225.2.2.2 only.

```
Switch# configure terminal
Switch(config)# ip access-list PIM-Control
Switch(config-ip-acl)# permit any host 225.2.2.2
Switch(config-ip-acl)# exit
Switch(config)# ip pim rp-address 10.90.90.90 group-list PIM-Control
Switch(config)#
```

79-11 ip pim rp-candidate

This command is used to configure the router as an RP candidate. Use the **no** form of this command to remove the router as candidate RP.

ip pim rp-candidate {*INTERFACE-ID* **[group-list** *ACCESS-LIST-NAME***] | interval** *SECONDS* **| priority** *PRIORITY* **| wildcard_prefix_cnt {0 | 1}}**

no ip pim rp-candidate *INTERFACE-ID*

Parameters

INTERFACE-ID	Specifies the interface ID. The IP address associated with this interface is advertised as a candidate RP address.
group-list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the standard IP access list that defines the group prefixes that are advertised in association with the RP address. If no group list is specified, the switch is a candidate RP for all groups.
interval *SECONDS*	Specifies the RP candidate advertisement interval. The range is from 1 to 16383 seconds. If not specified, default is 60 seconds.
priority *PRIORITY*	Specifies the RP priority value. The range is from 0 to 255. If not specified, default is 192.
wildcard_prefix_cnt	Specifies to set the wildcard (224.0.0.0/4) prefix count 1 or 0 in C-RP message. The default value is 0.

Default

The router is not an RP candidate by default.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only one group access list can be specified for each interface. This command only takes effect when the interface specified by the command is PIM-SM enabled. This command causes the router to send a PIMv2 message advertising itself as the candidate RP to the BSR.

Example

This example shows how to configure the router to advertise itself as the candidate RP to the BSR in its PIM domain. A basic IP access list, named PIM-Control, which specifies the group prefix (239.0.0.0/8), is associated with the RP that has the address identified by interface VLAN 1.

```
Switch# configure terminal
Switch(config)# ip access-list PIM-Control
Switch(config-ip-acl)# permit any 239.0.0.0 0.0.0.255
Switch(config-ip-acl)# exit
Switch(config)# ip pim rp-candidate vlan1 group-list PIM-Control
Switch(config)#
```

79-12 ip pim rp-register-kat

This command is used to configure the keep-alive time of (S, G) on the RP when receiving a register message. To restore the default value, use the **no** form of this command.

ip pim rp-register-kat *SECONDS*

no ip pim rp-register-kat

Parameters

SECONDS	Specifies the keep alive time, in the range from 1 to 65525 seconds.

Default

By default, this value is 185 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the DR receives multicast stream, it will send register message to the RP of the group. And when the RP receives this message, it would set up a timer for this (S, G) entry. This command configures the value of this timer.

Example

This example shows how to configure the PIM register keep-alive time to 500 seconds.

```
Switch# configure terminal
Switch(config)# ip pim rp-register-kat 500
Switch(config)#
```

79-13 ip pim spt-threshold

This command is used to configure the condition to switch over to the source tree. Use the **no** form of the command to revert to the default setting.

ip pim spt-threshold {0 | infinity}

no ip pim spt-threshold

Parameters

0	Specifies to establish the source tree right at the arrival of the first packet.
infinity	Specifies to always rely on the shared tree.

Default

By default, this option is **infinity**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command on the last hop of the router. In the PIM-SM mode, initially the multicast traffic from the source will be flowing along the RPT share tree to the receiver. After the first packet arrives at the last hop router, for each group of traffic, it can operate in one of the following two modes. With the mode

inifinity, the traffic keeps following the share tree. With the mode **0**, the source tree will be established and the traffic switchover to the source tree.

Example

This example shows how to set the SPT threshold to infinity.

```
Switch# configure terminal
Switch(config)# ip pim spt-threshold infinity
Switch(config)#
```

79-14 ip pim ssm

This command is used to configure the SSM multicast group address range. Use the **no** form of the command to disable PIM-SSM.

ip pim ssm {default | range *ACCESS-LIST***}**

no ip pim ssm

Parameters

default	Specifies to use the default SSM group addresses. The default SSM group address range is 232/8.
ACCESS-LIST	Specifies the standard IP access list that defines the user-specified SSM group addresses. The group address should be defined in the destination IP address field of the rule entry.

Default

By default, PIM-SSM is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only affects PIM-SM operation. Use this command on the last hop of the router only.

When SSM is enabled, the last hop router will initiate to establish a source-based tree for the channel (S,G) on receiving a IGMPv3 include (S, G) request that falls in the SSM range from the attached hosts.

Example

This example shows how to configure an IP standard access list and specifies the defined group address as the SSM range.

```
Switch# configure terminal
Switch(config)# ip access-list SSM-GROUP
Switch(config-ip-acl)# permit any 224.2.0.0 0.0.255.255
Switch(config-ip-acl)# exit
Switch(config)# ip pim ssm range SSM-GROUP
Switch(config)#
```

79-15 show ip pim

This command is used to display the PIM global information.

show ip pim

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the global information of PIM.

Example

This example shows how to display PIM global information.

```
Switch# show ip pim

PIM Configurations:

Register Checksum Wholepkt: (Not configured)
Register Probe Time            : 5 seconds
Register Suppression Time      : 60 seconds
Register Keepalive Time on RP  : 185 seconds
SPT Threshold                  : Infinity

RP Address
  90.1.1.1, group-list: static-rp

RP Candidate
  priority: 192, interval: 60 seconds, wildcard-prefix-cnt: 0
  vlan100, group-list: rp-cand

BSR Candidate
  vlan100, hash-mask-length: 30, priority: 1, interval: 60 seconds

SSM group : Movies

Switch#
```

79-16 show ip pim bsr-router

This command is used to display bootstrap router (BSR) information.

show ip pim bsr-router

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the elected BSR information and information about the locally configured candidate rendezvous point (RP) advertisement.

Example

This example shows how to display BSR information on the BSR router with the Candidate RP information on the router's interface, VLAN 100.

```
Switch# show ip pim bsr-router

PIMv2 Bootstrap information
This system is the Bootstrap Router (BSR)
  BSR address: 90.1.1.3
  BSR Priority: 3, Hash mask length: 30
  Next bootstrap message in 0DT00H00M21S
  Candidate RP: 90.1.1.3(vlan100), Group ACL: crp-list
    Next Cand_RP_advertisement in 0DT00H00M13S

Switch#
```

This example shows how to display BSR information on the non-BSR router with Candidate RP information on the router's interface

```
Switch# show ip pim bsr-router

PIMv2 Bootstrap information
  BSR address: 192.168.53.113
  BSR Priority: 255, Hash mask length: 30
  Next bootstrap message in 0DT00H02M04S
  Candidate RP: 192.168.38.111(loopback2), Group ACL: d235.1.3-4/24
    Next Cand_RP_advertisement in 0DT00H00M41S

Switch#
```

79-17 show ip pim interface

This command is used to display the interface information.

show ip pim interface [dense-mode | sparse-mode | sparse-dense-mode] [*INTERFACE-ID*] [detail]

Parameters

INTERFACE-ID	(Optional) Specifies the interface which to display the interface information. Only VLAN interface IDs are applicable.
detail	(Optional) Specifies to display the interface information in detail.
dense-mode	(Optional) Specifies to display information only for PIM dense-mode
sparse-mode	(Optional) Specifies to display information only for PIM sparse-mode
sparse-dense-mode	(Optional) Specifies to display information only for PIM sparse-dense-mode

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display interface related information. If no interface is specified, the PIM information for all applicable interfaces will be shown.

Example

This example shows how to display interface information.

```
Switch# show ip pim interface

p: passive, Nbr Cnt: Neighbor Count

Address         Interface  Mode   Nbr DR      DR              Generation
                                  Cnt Priorty                 ID
--------------- ---------- ------ --- ------- --------------- ----------
90.1.1.1        vlan100    SM(p)  0   1       90.1.1.1        1645d8a00
30.1.1.1        vlan200    DM     1   0       0.0.0.0         3a5f93
12.1.1.1        vlan300    SM-DM  1   0       0.0.0.0         37c693

Total Entries: 3

Switch#
```

This example shows how to display interface information in detail.

```
Switch# show ip pim interface detail

vlan100
  Address                  : 90.1.1.1
  PIM                      : Enabled
  Mode                     : Sparse
  Neighbor Count           : 1
```

```
  DR                        : 90.1.1.1
  DR Priotity               : 1
  Generation ID             : 1645d8a00
  Hello Interval            : 30 seconds
  Join Prune timer          : 60 seconds
  PIM Passive Mode          : Disabled

vlan200
  Address                   : 50.111.111.111
  PIM                       : Enabled
  Mode                      : Dense
  Neighbor Count            : 0
  Generation ID             : 3a5f93
  Hello Interval            : 30 seconds
  PIM Passive Mode          : Enabled

vlan300
  Address                   : 12.1.1.1
  PIM                       : Enabled
  Mode                      : Sparse-Dense
  Neighbor Count            : 0
  DR                        : 12.1.1.1
  DR Priority               : 1
  Generation ID             : 9e3d65
  Hello Interval            : 30 seconds
  Join Prune Timer          : 60 seconds
  PIM Passive Mode          : Disabled

Total Entries: 3

Switch#
```

79-18 show ip pim neighbor

This command is used to display the PIM-SM neighbor information.

show ip pim neighbor [*INTERFACE-ID***]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface to display PIM-SM neighbor information. If the interface ID is not configured, information on all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to determine which routers on the LAN are configured for PIM.

Example

This example shows how to display the PIM neighbor information on all interfaces.

```
Switch# show ip pim neighbor

Mode: DR - Designated Router, N - Default DR Priority,
      G – Generation ID
Neighbor        Interface  Uptime/Expires            Ver            DR Pri/Mode
--------------------------------------------------------------------------------
10.10.0.9       vlan1      0DT00H55M33S/0DT00H01M44S  v2             1 /G
10.10.0.136     vlan1      0DT00H55M20S/0DT00H01M25S  v2             1 /G
10.10.0.172     vlan1      0DT00H55M33S/0DT00H01M32S  v2             1 /DR,G
192.168.0.100   vlan2      0DT00H55M30S/0DT00H01M20S  v2             N /G

Total Entries: 4

Switch#
```

79-19 show ip pim rp mapping

This command is used to display group-to-RP (rendezvous point) mappings and the RP set.

show ip pim rp mapping

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display active rendezvous points (RPs) that are cached with associated multicast routing entries. This command is used to display the RP mapping information viewed by the router

Example

This example shows how to display group-to-RP (rendezvous point) mappings and the RP set.

```
Switch# show ip pim rp mapping

Group(s): 224.0.0.0/4
RP: 90.1.1.3
Info source: 90.1.1.3, via bootstrap, priority 0
```

```
Uptime: 0DT16H52M39S, expires: 0DT00H02M50S
Group(s): 225.0.0.0/8
RP: 1.1.1.10
Info source: static

Switch#
```

Display Parameters

RP	The address of the RP for the group specified.
Info source	Indicates from which system the router learned this RP information.
Via bootstrap	The RP mapping information is learned from the BSR.
Priority	The RP priority.
Uptime	The length of time (in day, hours, minutes, and seconds) that the router has known about this RP.
Expires	The time (in day, hours, minutes, and seconds) after which the information about this RP expires. If the router does not receive any refresh messages in this time, it will discard information about this RP.

79-20 show ip pim rp-hash

This command is used to display the rendezvous point (RP) to be chosen based on the group selected.

show ip pim rp-hash *GROUP-ADDRESS*

Parameters

GROUP-ADDRESS	Specifies the group address to display the selected RP for the group.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the RP selected for the specified group.

Example

This example shows how to display the RP with the group address 238.10.10.10.

```
Switch# show ip pim rp-hash 238.10.10.10

RP: 10.20.30.1
Info source: 10.20.30.1, via bootstrap
Uptime: 0DT01H42M15S, expires: 0DT00H02M16S
```

```
Switch#
```

This example shows how to display the RP with the group address 225.1.1.1.

```
Switch#show ip pim rp-hash 225.1.1.1

RP: 1.1.1.10
Info source: static

Switch#
```

80. Protocol Independent Commands

80-1 distance

This command is used to define an administrative distance for static routes. Use **no** command to revert to the default setting.

distance [vrf *VRF-NAME***] {static | default}** *DISTANCE*

no distance [vrf *VRF-NAME***] {static | default}**

Parameters

vrf *VRF-NAME*	(Optional) Specifies the VRF routing process.
static	Specifies the administrative distance of static routes.
default	Specifies the administrative distance of static default routes.

Default

The default distance of a static route is 60.

The default distance of a static default route is 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the distance is an integer from 0 to 255 representing the trust rating of the route. The route with a lower distance value is preferred over the route with a higher distance value. A route with the distance 255 will not be installed for routing of packets since it indicates that the route is not trusted. If the distance command is used without parameters, the specified distance becomes the default value for routes of the configured protocol.

Example

This example shows how to configure the static route distance to 100.

```
Switch# configure terminal
Switch(config)# distance static 100
Switch(config)#
```

80-2 distribute-list

This command is used to configure the distribute list which filters the protocol route updates based on the specified access list.

distribute-list *ACCESS-LIST-NAME* **in [***INTERFACE-ID***]**

no distribute-list *ACCESS-LIST-NAME* **in [***INTERFACE-ID***]**

Parameters

ACCESS-LIST-NAME	Specifies a standard IP access list to define which received route updates are to be accepted and which route updates are to be advertised.
INTERFACE-ID	(Optional) Specifies the interface to apply the distribute list.
in	Specifies to apply the distribute list to incoming route updates.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the access list is applied to the interface using the distribute-list in command, the route updates received by the specified interface will be filtered based on the access list.

If the interface ID is specified, the distribute-list is applied to the specified interface. If the interface ID is not specified, the distribute list is applied to all interfaces.

Example

This example shows how to configure access list “East-ranch” to filter RIP protocol route updates.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# distribute-list East-ranch in
Switch(config-router)#
```

80-3 ip prefix-list

This command is used to create a prefix list entry. Use the **no** form of this command to delete a prefix list entry.

ip prefix-list *LIST-NAME* **{[seq** *NUMBER***] {deny | permit}** *NETWORK-ADDRESSIMASK-LENGTH* **[ge** *GE-LENGTH***] [le** *LE-LENGTH***] | description** *DESCRIPTION***}**

no ip prefix-list *LIST-NAME* **{seq** *NUMBER* **| description}**

Parameters

LIST-NAME	Specifies the prefix list’s name. The maximum length is 32 bytes.
seq *NUMBER*	(Optional) Specifies the sequence number The range is from 1 to 65535. The lower the number is, the higher the precedence of the permit/deny rule.
permit	Specifies that routes that match the entry are permitted.
deny	Specifies that routes that match the entry are denied.
NETWORK-ADDRESSIMASK-LENGTH	Specifies a network address and the length of the mask bit.

GE-LENGTH	(Optional) Specifies the minimum prefix length of the route that can be matched.
LE-LENGTH	(Optional) Specifies the maximum prefix length of the route that can be matched.
DESCRIPTION	Specifies the description for prefix list.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 5 is assigned. A subsequent rule entry will be assigned a priority that is 5 greater than the largest sequence number in that access list and is placed at the end of the list.

When manually assigning 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 priority value that is already present, the new entry will override the old one.

Only the route that is equal to or more specific than the specified network will be matched.

Example

This example shows how to create 2 rule entries, the first is to exactly match with 10.20.0.0/16, the second is to permit routes from the 10.50.0.0/16 that have a mask length that is less than or equal to 24 bits.

```
Switch# configure terminal
Switch(config)# ip prefix-list CUSTOMER permit 10.20.0.0/16
Switch(config)# ip prefix-list CUSTOMER seq 20 permit 10.50.0.0/16 le 24
Switch(config)#
```

80-4 ip route

This command is used to create a static route entry. Use **no** command to remove a static route entry.

ip route [vrf *VRF-NAME***] {***NETWORK-PREFIX NETWORK-MASK***} {***IP-ADDRESS* **[primary | backup | weight** *NUMBER***] | null0 |** *TUNNEL-INTERFACE-ID***}**

no ip route [vrf *VRF-NAME***] {***NETWORK-PREFIX NETWORK-MASK***} {***IP-ADDRESS* **| null0 |** *TUNNEL-INTERFACE-ID***}**

Parameters

VRF-NAME	(Optional) Specifies the name of the routing forwarding instance.
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.
weight *NUMBER*	(Optional) Specifies the weight number greater than zero, but less than the maximum paths number. This number is used to replicate identical route path (multiple copies) in routing table, so the path get more chance to be hit for traffic routing. If weight number is not specified for the static route, the default for the path exists in hashing table is one copy.
null0	Specifies a black hole route.
TUNNEL-INTERFACE-ID	Specifies to use a tunnel as the next-hop.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If a static route entry is configured with weight greater than 1, then the entry will be replicated multiple copies in the hashing table so the path gets more chance to be hit for traffic routing. When the total number of replication exceeds the maximum paths number supported by the hardware platform, the ordering in which the static route is configured determines the precedence.

If null0 is specified for one route, the traffic that matched its destination will be dropped.

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)#
```

80-5 ipv6 route

This command is used to create an IPv6 static route entry. Use the **no** command to remove an IPv6 static route entry.

ipv6 route {default | *NETWORK-PREFIXIPREFIX-LENGTH***} {[***INTERFACE-ID***]** *NEXT-HOP-ADDRESS* **[primary | backup] [***DISTANCE***] |** *TUNNEL-INTERFACE-ID***}**

no ipv6 route {default | *NETWORK-PREFIXIPREFIX-LENGTH***} {[***INTERFACE-ID***]** *NEXT-HOP-ADDRESS* **|** *TUNNEL-INTERFACE-ID***}**

Parameters

default	(Optional) Specifies to add or delete a default route.

NETWORK-PREFIXIPREFIX-LENGTH	(Optional) Specifies the network prefix and the prefix length of the static route.
NEXT-HOP-ADDRESS	(Optional) 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 route to the destination.
backup	(Optional) Specifies the route as the backup route to the destination.
DISTANCE	(Optional) Specifies the administrative distance of the static route. The range of distance is 1 to 255. The lower value represents better route. If not specified, the default administrative distance for a static route is 1.
TUNNEL-INTERFACE-ID	(Optional) Specifies to use a tunnel as the next-hop.
INTERFACE-ID	(Optional) Specifies the forwarding interface for routing the packet.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The distance of routes is used in the following ways. There are a number of sources that a route can be learned from. Each route is associated with a distance. The route with the least distance will be installed in routing table.

If multiple routes to the same destination network is configured with the same distance, and the distance is less than distance of routes learned from other sources, then these routes will be installed in the routing table simultaneously, and the traffic is distributed among these paths in parallel. This is referred to ECMP (equal cost multiple paths). The installed parallel routes must belong to the same protocol.

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)#
```

80-6 ip route ecmp load-balance

This command is used to configure the load balancing hash key used to determine the next hop entry from the multiple paths destined for the same destination. Use the **no** form of the command to return to default setting.

ip route ecmp load-balance [{sip | crc32_lower | crc32_upper} | dip | port]

no ip route ecmp load-balance [{sip | crc32_lower | crc32_upper} | dip | port]

Parameters

sip	(Optional) Specifies to include the source IP address in the hash value computation.
crc32_lower	(Optional) Specifies to include the lower 5 bits of the CRC in the hash value computation.
crc32_upper	(Optional) Specifies to include the upper 5 bits of the CRC in the hash value computation.
dip	(Optional) Specifies to include the destination IP address in the hash value computation.
port	(Optional) Specifies to include the TCP/UDP port number in the hash value computation.

Default

By default, this option is **sip**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When a route has multiple paths in the routing table going to the same destination, the system will take the next hop entry based on the hashing result. Use the **ip route ecmp load-balance** command to define the data which will be included in the hash value computation. The source IP address is always included in the hash value computation. This command issued later will overwrite the previous command setting.

Example

This example shows how to include the destination IP address and port number in the hash value computation.

```
Switch# configure terminal
Switch(config)# ip route ecmp load-balance dip
Switch(config)#
```

80-7 maximum-paths

This command is used to specify the maximum number of parallel routes of the configured routing protocol which can be installed in the routing table simultaneously. Use the **no** form of the command to revert to the default setting.

maximum-paths *NUMBER-PATHS*

no maximum-paths

Parameters

NUMBER-PATHS	Specifies the maximum number of parallel routes of an IP routing protocol that can be installed in the routing table. The minimum number is 1.

Default

By default, this value is 1.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

There are a number of sources that a route can be learned from. Each route is associated with a distance. The route with the least distance will be installed in routing table.

The value of maximum paths determines the maximum number of parallel routes to the same destination network learned from the configured protocol that can be installed in the routing table simultaneously .The installed parallel routes must belong to the same source.

Example

This example shows how to configure the maximum paths of the OSPF protocol to 3.

```
Switch# configure terminal
Switch(config)# router ospf
Switch(config-router)# maximum-paths 3
Switch(config-router)#
```

80-8 show ip prefix-list

This command is used to display the configured prefix lists.

show ip prefix-list [*PREFIX-LIST-NAME***]**

Parameters

PREFIX-LIST-NAME	(Optional) Specifies to display the entries of prefix list in specified prefix list.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the IPv4 prefix list setting.

Example

This example shows how to display all of the configured IPv4 prefix lists.

```
Switch# show ip prefix-list

ip prefix-list customer-prefix:
Description: This prefix list is used for East-Branch.
count: 2
Seq 5 permit 10.20.0.0/16
```

```
Seq 10 permit 20 10.50.0.0/16 le 24

Total Entries: 1

Switch#
```

80-9 show ip protocols

This command is used to display the state of the routing process.

show ip protocols [rip | ospf | bgp] [vrf *VRF-NAME***]**

Parameters

rip	(Optional) Specifies to display the RIP protocol overall configuration.
ospf	(Optional) Specifies to display the OSPF protocol overall configuration.
bgp	(Optional) Specifies to display the BGP protocol overall configuration.
vrf *VRF-NAME*	(Optional) Specifies to display the VRF routing process.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the status of the routing processes. If no option is specified, all running routing processes are displayed.

Example

This example shows how to display the routing protocol information.

```
Switch# show ip protocols

Routing Protocol is RIP
  Sending updates every 5 seconds, next due in 5 seconds
  Invalid 180 secs,  flush 120 secs
  Default redistribution metric is 0
  Redistributing : OSPF,static,connected,BGP,
  Default version control: send version 1, receive any version
    Interface     Send       Recv
    vlan10        1          1 2
    vlan20        1          1 2
    vlan40        1          1 2
    vlan70        1          1 2
    vlan8         1          1 2
    vlan11        1          1 2
    vlan1         1          1 2
```

```
    vlan31        1          1 2
    vlan32        1          1 2
    vlan33        1          1 2
  Routing for Networks:
    vlan10  (1.0.0.1/255.0.0.0)
    vlan20  (2.0.0.1/255.0.0.0)
    vlan40  (4.0.0.1/255.0.0.0)
    vlan70  (7.0.0.3/255.0.0.0)
    vlan8   (8.0.0.1/255.0.0.0)
    vlan11  (11.0.0.1/255.0.0.0)
    vlan1   (40.90.90.90/255.0.0.0)
    vlan31  (131.0.0.1/255.255.0.0)
    vlan32  (132.0.0.1/255.255.0.0)
    vlan33  (133.0.0.1/255.255.0.0)
  Routing Information Sources:
    Gateway          Last Update
    1.0.0.2          01:22:25
    2.0.0.2          01:22:25
    131.0.0.2        01:22:25
    132.0.0.2        01:22:25
    133.0.0.2        01:22:25
  Distribute list:
    East branch (in)
    Interface   in
    vlan20       East branch-acl1
  Distance:100

Routing Protocol is OSPF
Router ID 222.200.23.1
It is an area boundary router
It is an autonomous system boundary router
Redistributing external route from
  RIP with metric mapped to 20
  Static with metric mapped to 20
  Connected with metric mapped to 20
  BGP with metric mapped to 20
Number of areas in this router is 5. 5 normal, 0 stub, 0 nssa
Maximum path: 32.
Routing for network:
    40.90.90.90/8
    8.0.0.1/8
    1.0.0.1/8
    11.0.0.1/8
    2.0.0.1/8
    131.0.0.1/16
    132.0.0.1/16
    133.0.0.1/16
    4.0.0.1/8
    7.0.0.3/8
Routing Information Sources:
    Gateway
    1.0.0.2
    2.0.0.2
    4.0.0.2
```

```
    7.255.255.254
    8.0.0.2
    11.0.0.2
    131.0.0.2
    132.0.0.2
    133.0.0.2
    4.0.0.2
Distribute list:
  vlan1 filtered by abc.
  vlan8 filtered by abc.
  vlan11 filtered by abc.
External-1 Distance 110,External-2 Distance 115,inter-area distance 90, intra-area
distance 80.

Routing Protocol is "BGP 1"
  Router ID 222.200.23.1
  IGP synchronization is disabled
  Redistributing:
  Default local preference is 100
  Aggregated network(s)
  Neighbor(s)
  Maximum path: 1
  External distance 70, internal distance 130

Switch#
```

80-10 show ip route

This command is used to display the entry in the routing table.

show ip route [vrf *VRF-NAME***] [[***IP-ADDRESS* **[***MASK***] | *PROTOCOL***] | hardware]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies to display the VRF routing table.
IP-ADDRESS	(Optional) Specifies the network address of which routing information should be displayed.
MASK	(Optional) Specifies the subnet mask for the specified network.
PROTOCOL	(Optional) Specifies the routing protocol, or the following keywords: static, connected.
hardware	(Optional) Specifies to display the routes that have been written into chip.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The routing table gathers routes learned from different protocols. If multiple routes can reach the same network, the one with the best distance and the next hop is reachable will be chosen as the best and set to hardware for routing of packets. They are the route entry currently at work. That is, if the route with the best distance is with the unreachable next hop, then the route with the next preferred distance will be chosen.

Example

This example shows how to display the routing table.

```
Switch# show ip route

Codes: C - connected, S - static, R - RIP, B - BGP O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2,
       * - candidate default

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

O E2 10.110.0.0/8   [160/5] via 10.119.254.6, vlan2,  0DT0H1M
R     10.67.10.0/8   [200/128]  via 10.119.254.244, vlan2, 0DT0H2M22S
O E2 10.68.132.0/8 [160/5]    via 10.119.254.6,  vlan2,  0DT0H0M59S
O E2 10.130.0.0/8  [160/5]    via 10.119.254.6,   vlan2, 0DT0H0M59S
R     10.128.0.0/8   [200/128] via 10.119.254.244, vlan2, 0DT0H2M22S
R     10.129.0.0/8   [200/129] via 10.119.254.240, vlan2, 0DT0H2M22S
R     10.65.129.0/8 [200/128] via 10.119.254.244, vlan2, 0DT0H2M22S
R     10.10.0.0/8    [200/128] via 10.119.254.244, vlan2, 0DT0H2M22S
R     10.75.139.0/8 [200/129] via 10.119.254.240, vlan2, 0DT0H2M23S
R     10.16.208.0/8 [200/128] via 10.119.254.244, vlan2, 0DT0H2M22S
R     10.84.148.0/8 [200/129] via 10.119.254.240, vlan2 0DT0H2M23S
R     10.31.223.0/8 [200/128] via 10.119.254.244, , vlan2 0DT0H2M22S

Total Entries: 11 entries, 11 routes

Switch#
```

Display Parameters

Code	Indicates the source type that the route is derived from. It can be one of the following values: C - Connected. S - Static. R - Routing Information Protocol (RIP) derived. B - Border Gateway Protocol (BGP) derived. O - Open Shortest Path First (OSPF) derived. C - Connected.
Sub Code	The type of route. It can be one of the following values: IA - OSPF interarea route. E1 - OSPF external type 1 route. E2 - OSPF external type 2 route.

	N1 - OSPF not-so-stubby area (NSSA) external type 1 route. N2 - OSPF NSSA external type 2 route.
*****	The candidate default.
^	The next hop is reachable.
>	The route with the best distance among routes learned from multiple protocols.
P	The stale route during restarting of protocols.
10.110.0.0/8	Indicates the network.
[160/5]	The first number is the administrative distance of the protocol source; the second number is the metric for the route.
via 10.119.254.6	Specifies the next hop to the network.
0DT0H1M	Specifies the time since last update in [n]DT[n]H[n]M[n]S.
Vlan2	Specifies the interface through which the specified network can be reached.

80-11 show ip route summary

This command is used to display the brief information for the working routing entries.

show ip route summary [vrf *VRF-NAME***]**

Parameters

vrf *VRF-NAME*	(Optional) Specifies to display the VRF routing table.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays 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       2
Static          0
RIP             1
OSPF            0
```

```
BGP             2
Total           5
Multi-path      0

Switch#
```

80-12 show ipv6 route

This command is used to display the entry in routing table.

show ipv6 route {[*IPV6-ADDRESS* **|** *NETWORK-PREFIXIPREFIX-LENGTH* **[longer-prefixes] |** *INTERFACE-ID* **|** *PROTOCOL*] **[database] | hardware}**

Parameters

IPV6-ADDRESS	(Optional) Specifies an IPv6 address to find a longest prefix matched IPv6 route.
NETWORK-PREFIX	(Optional) Specifies the network address of which routing information should be displayed.
PREFIX-LENGTH	(Optional) Specifies the prefix length for the specified network
longer-prefixes	(Optional) Specifies to display the route and all of the more specific routes.
INTERFACE-ID	(Optional) Specifies the interface type.
PROTOCOL	(Optional) Specifies the routing protocol.
hardware	Specifies to display the routes that have been written into chip.
database	(Optional) Specifies to display all the related entries in the routing database instead of just the best route.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The routing table gathers routes learned from different protocols. If multiple routes can reach the same network, the one with the best distance and the next hop is reachable will be chosen as the best and set to hardware for routing of packets. They are the route entry currently at work. That is, if the route with the best distance is with the unreachable next hop, then the route with the next preferred distance will be chosen.

Example

This example shows how to display the routing entries for IPv6.

```
Switch# show ipv6 route

IPv6 Routing Table
```

```
Code: C - connected, S - static, R - RIP, O - OSPF,
      IA - OSPF inter area
      E1 - OSPF external type 1, E2 - OSPF external type 2
      SLAAC - Stateless address autoconfiguration

S     ::/0 [1/1] via 1001::2, vlan10
C     1001::/64 [0/1] is directly connected, vlan10
O IA  1005::/64 [110/20] via FE80::2C0:8FFF:FE04:1128, vlan10
O IA  1005::1/128 [110/10] via FE80::2C0:8FFF:FE04:1128, vlan10
O IA  1005::2/128 [110/20] via FE80::2C0:8FFF:FE04:1128, vlan10
O IA  1006::/64 [110/20] via FE80::208:62FF:FE02:302, vlan40
C     1007::/64 [0/1] is directly connected, vlan70
C     1008::/64 [0/1] is directly connected, vlan8
O     1009::/64 [110/20] via FE80::2C0:8FFF:FE04:1128, vlan10
C     1011::/64 [0/1] is directly connected, vlan11
O     1012::/64 [110/20] via FE80::202:FF:FE00:0, vlan11
O IA  1017::/64 [110/20] via FE80::2C0:8FFF:FE04:1128, vlan10
R     2100::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:1::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:2::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:3::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:4::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:5::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:6::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:7::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:8::/64 [120/2] via FE80::1, vlan70
R     2100:0:0:9::/64 [120/2] via FE80::1, vlan70
C     2131::/64 [0/1] is directly connected, vlan31
C     2132::/64 [0/1] is directly connected, vlan32
C     2133::/64 [0/1] is directly connected, vlan33
S     300A::/64 [1/1] via 1001::2, vlan10
C     3600::/64 [0/1] is directly connected, vlan1
O     3620::/64 [110/20] via FE80::2C0:8FFF:FE04:1128, vlan10
O     4000::/64 [110/10] via FE80::208:62FF:FE02:302, vlan40
O     4000::A/128 [110/10] via FE80::208:62FF:FE02:302, vlan40
S     400B::/64 [1/1] via FD20:1305:815:20:286:53FF:FE62:7F03, vlan20
C     FD01::/48 [0/1] is directly connected, vlan10
C     FD20:1305:815:20::/64 [0/1] is directly connected, vlan20
C     FD80::/9 [0/1] is directly connected, vlan40

Total Entries: 34 entries, 34 routes

Switch#
```

Display Parameters

Code	Indicates the source type that the route is derived from. It can be one of the following values: C - Connected. S - Static. R - Routing Information Protocol (RIP) derived. O - Open Shortest Path First (OSPF) derived.

	C - Connected.
Sub-Code	IA - OSPF inter-area route. E1 - OSPF external type 1 route. E2 - OSPF external type 2 route.
*****	The next hop is reachable.
>	The route with the best distance among routes learned from multiple protocols.
115:50:70::/64	Indicates the network.
[110/2]	The first number is the administrative distance of the protocol source; the second number is the metric for the route.
via fe80::a00:1ff:fe02:6	Specifies the next hop to the network.
vlan10	Specifies the interface through which the specified network can be reached.

80-13 show ipv6 route summary

This command is used to display the current state of the IPv6 routing table.

show ipv6 route summary

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 current state of the IPv6 routing table.

```
Switch# show ipv6 route summary

Route Source    Networks
Connected       2
Static          0
RIPng           1
OSPF            0
Total           3

Switch#
```

81. QoS Amendment Data Center Bridge (DCB) Commands

81-1 class type network-qos

This command is used to specify the name of the type network Quality of Service (QoS) class map to be associated with a traffic policy and then enter into the policy-map type network QoS class configuration mode.

class type network-qos *NAME*

Parameters

NAME	Specifies the name of the class map to be associated with a traffic policy.

Default

None.

Command Mode

Policy-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The type of network QoS is used for the switch that supports the DCB function. If the specified name of class map does not exist, no traffic is classified to the class. A warning message will be prompted to indicate it.

Use the **policy-map type network-qos global configuration** command to identify the policy map (type of network QoS) and enter the policy map configuration mode.

Example

This example shows how to create a network QoS class map to classify the traffic that match priority is 1, 3 or 5.

```
Switch# configure terminal
Switch(config)# class-map type network-qos match-any my_class_map
Switch(config-cmap-nq)# match cos 3
Switch(config-cmap-nq)# match cos 1
Switch(config-cmap-nq)# match cos 5
Switch(config-cmap-nq)# exit
Switch(config)# policy-map type network-qos my_policy_map
Switch(config-pmap-nq)# class type network-qos my_class_map
Switch(config-pmap-c-nq)# pause
Switch(config-pmap-c-nq)#
```

81-2 class-map type network-qos match-any

This command is used to create or modify a type network QoS class map that defines the criteria for packet matching.

class-map type network-qos match-any *NAME*

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The global configuration command **class-map type network-qos match-any** is used to specify the name of the type network QoS class map to create or modify class map match criteria and if multiple match statements in the class map will be evaluated based on the logical OR. The **class-map type network-qos match-any** command and its sub-commands are used to define packet classification. This command enters the class-map configuration mode.

Use the following commands to define or modify the match criteria:

- **match cos:** To define the class of traffic in a type network QoS class map, use the match cos command.
- **no match cos:** Removes a match statement from a class map.

Example

This example shows how to create a type network QoS class map, named “my_class_map”.

```
Switch# configure terminal
Switch(config)# class-map type network-qos match-any my_class_map
Switch(config-cmap-nq)#
```

81-3 ets-queue bandwidth

This command is used to assign the bandwidth to every traffic class. To restore to the default setting, use the **no** form of this command.

ets-queue bandwidth *WEIGHT1...WEIGHT100*

no ets-queue bandwidth

Parameters

WEIGHT1...WEIGHT100	Specifies the ETS bandwidth weight from 0 to 100 for each COS queue (traffic class). These values are the percentage of the available bandwidth assigned to a traffic class. WEIGHT1 for traffic class 0, WEIGHT2 for traffic class 1, and so on. The sum of the bandwidths assigned to a given port is required at all times to be equal to 100. The

number of zero stands for strict priority mode.

Default

By default, 4, 7, 11, 14, 18, 21, 25 (in percentage) are assigned for Traffic Classes 0 to 6.

By default, 0 is assigned for Traffic Class 7 which means that the transmission selection algorithm is “strict priority”.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The ETS bandwidth assignment only takes effect when the scheduling mode is ETS.

Example

This example shows how to assign available bandwidth to traffic classes for the ETS scheduling mode on interface eth1/0/3. This example allocates 10%, 20%, 30%, and 40% available bandwidth to traffic classes 0 to 3. Assign traffic class 4 to 7 to strict priority.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# mls qos scheduler ets
Switch(config-if)# ets-queue bandwidth 10 20 30 40 0 0 0 0
Switch(config-if)#
```

81-4 mls qos scheduler ets

This command is used to configure the queue scheduling to the Enhanced Transmission Selection (ETS) mode.

mls qos scheduler ets

Parameters

None.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

ETS is defined in IEEE 802.1Qaz. ETS provides an operational model for priority processing and bandwidth allocation in the switches in a DCB environment. Using priority-based processing and bandwidth allocations, different traffic classes with different types of traffic such as LAN, Storage Networking, Clustering, and management can be configured to provide bandwidth allocation or best effort

transmit characteristics. When the offered load in the traffic class doesn't use its allocated bandwidth, ETS will allow other traffic classes to use the available bandwidth. The bandwidth assigned to each traffic class is configured in unit of percentage by the **ets-queue bandwidth** command.

Example

This example shows how to configure the queue scheduling algorithm mode to ETS mode on interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# mls qos scheduler ets
Switch(config-if)#
```

81-5 pause

This command is used to enable Priority-based Flow Control (PFC) on a class referenced in a type network QoS policy map. Use the **no** form of the command to disable Priority-based Flow Control (PFC) on a class.

pause

no pause

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Policy Map Type Network-QoS Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Ethernet interfaces use Priority-based Flow Control (PFC) to provide lossless service.

PFC, which is defined in IEEE 802.1Qbb, extends the basic IEEE 802.3x PAUSE semantics and uses the IEEE 802.1p CoS values in the IEEE 802.1Q VLAN tag to differentiate up to eight CoSs that can be subject to flow control independently.

If PFC of all priorities is disabled, the interface defaults to the IEEE 802.3x flow control setting. When PFC of any priority is enabled, the interface will recognize PFC PAUSE frames. In other words, the switch will pause a CoS on which PFC is enabled and the received PFC PAUSE indicates the CoS should be paused. A PFC PAUSE frame will be transmitted if the congestion is detected on the PFC enabled CoS.

To enable PFC on a per-CoS basis, do the following:

- Use the **class-map type network-qos match-any global configuration** command to create a type network QoS class map.
  - Use the **match cos class-map configuration** command to specify which CoS to configure.
- Use the **policy-map type network-qos** command to create a type network QoS policy map.
  - Use the **class type network-qos policy-map configuration** command to specify a type network QoS class map to be associated with a traffic policy and then enter into the policy-map type network-QoS class configuration mode.

    - Use the **pause policy map type network-qos class configuration** command to enable PFC pause characteristics on a class referenced in a type network QoS policy map.
- Use the **service-policy type network-qos input interface configuration** command to apply a type network QoS policy map.

Example

This example shows how to enable PFC on priority 3 and 4 at interface eth1/0/3.

Step 1: Create a type network QoS class map, named “my_class_map” and set the criteria to match CoS 3 or 4.

```
Switch# configure terminal
Switch(config)# class-map type network-qos match-any my_class_map
Switch(config-cmap-nq)# match cos 3
Switch(config-cmap-nq)# match cos 4
Switch(config-cmap-nq)#
```

Step 2: Create a type network QoS policy map, named “my_policy_map” and enable PFC for the class, “my_class_map”, which is created in step 1.

```
Switch# configure terminal
Switch(config)# policy-map type network-qos my_policy_map
Switch(config-pmap-nq)# class type network-qos my_class_map
Switch(config-pmap-c-nq)# pause
Switch(config-pmap-c-nq)# exit
Switch(config-pmap)#
```

Step 3: Apply the type network QoS policy map, “my_policy_map”, created in step 2, on interface eth1/0/3.

```
Switch# configure terminal
Switch(config)# interface eth1/0/3
Switch(config-if)# service-policy type network-qos input my_policy_map
Switch(config-if)#
```

81-6 policy-map type network-qos

This command is used to enter the policy-map configuration mode and create or modify a type network QoS policy map that can be attached to one or more interfaces as a type network QoS service policy.

policy-map type network-qos *NAME*

Parameters

NAME	Specifies the name of the type network QoS policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **policy-map type network-qos** command to enter the policy-map configuration mode from where to configure or modify the policy for the traffic class.

Use the **class-map type network-qos match-any** and **match cos** commands to configure the match criteria for a class.

A single policy map can be attached to more than one interface concurrently. The succeeding policy-map type network QoS attached overwrites the previous one.

In the type network QoS policy map configuration mode, use the following commands to attach or detach the class map to/from the policy map:

- **class type network-qos:** Attach a type network QoS class map that defined classification criteria to the policy map and enter the policy map type network QoS class configuration mode.
- **no class:** Remove a class map from this policy map.

The type network QoS policy maps may contain more than one traffic class by using the **class type network-qos policy-map** configuration command.

Attach the type network QoS policy map to an interface at the ingress by using the **service-policy type network-qos input interface configuration** command.

Example

This example shows how to create a type network QoS policy map and modify the PFC state for the class-map.

```
Switch# configure terminal
Switch(config)# policy-map type network-qos my_policy_map
Switch(config-pmap-nq)# class-map type network-qos my_class_map
Switch(config-pmap-c-nq)# pause
Switch(config-pmap-c-nq)# exit
Switch(config-pmap-nq)# class-map type network-qos my_class_map_pfc_off
Switch(config-pmap-c-nq)# no pause
Switch(config-pmap-c-nq)#
```

81-7 service-policy type network-qos input

This command is used to attach a type network QoS policy map to an input interface.

service-policy type network-qos input *NAME*

Parameters

NAME	Specifies the name of a type network QoS service policy map (created by the **policy-map type network-qos** command) to be attached. The name can be a maximum of 32alphanumeric characters.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **service-policy type network-qos** command to attach a single type network QoS policy map to input interfaces. A policy map need not be created before specifying it in this command. A command will not take effect when it associates a non-existent service policy. If there is no statement in the policy map, nothing will be performed.

Besides a single policy map (without specifying type name) for each type (input or output) on an interface, up to one type network QoS policy map can be applied on a physical port interface at input (ingress).

Example

This example shows how to apply the policy map policy1 to a physical ingress interface.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# service-policy type network-qos input my_policy_map
Switch(config-if)#
```

81-8 show class-map type network-qos

This command is used to display the type network QoS class map configuration.

show class-map type network-qos [*NAME***]**

Parameters

NAME	(Optional) Specifies the name of the class map. The class map name can be a maximum of 32alphanumeric characters.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use the **show class-map type network-qos** command to display the type network QoS class maps. If the optional *NAME* argument is entered, the specified type network QoS class map and its matching criteria will be displayed.

Example

This example shows how to display all type network QoS class maps.

```
Switch# show class-map type network-qos

Type network-qos class-maps
===========================
Class Map my_class_map
match cos 3,4

Class Map my_class_map_2
  match cos 2
```

```
Class Map my_class_map_3
  match cos 5

Switch#
```

81-9 show mls qos queuing interface

This command is used to display the weight configuration for different scheduler algorithms on specified interface(s).

show mls qos queuing interface *INTERFACE-ID* **[,|-]**

Parameters

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

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the bandwidth assignment for all scheduling modes.

Example

This example shows how to display the queuing information on interface eth3/0/1.

```
Switch# show mls qos queuing interface eth3/0/1

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  Quantums
```

```
  ---  -------
   0      1
   1      2
   2      3
   3      4
   4      5
   5      6
   6      7
   7      8
ETS bandwidth weights:
QID     Percentages
  ---     ------------------
   0      10
   1      20
   2      30
   3      40
   4      strict priority
   5      strict priority
   6      strict priority
   7      strict priority

Switch#
```

81-10 show policy-map interface

This command is used to display the policy map configuration on the specified interface.

show policy-map interface *INTERFACE-ID*

Parameters

INTERFACE-ID	Specifies the interface ID.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the policy maps configuration, if any, that has been attached to the specified interface.

Example

This example shows how to displays the policy maps configuration, if any, that has been attached to the specified interface.

```
Switch# show policy-map interface eth3/0/1
```

```
Policy Map: policy1(network-qos) : input
Class Map my_class_map_2

pause
Policy Map: policy2 : input
  Class police
police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-dscp-transmit 2
violate-action drop

Switch#
```

81-11 show policy-map type network-qos

This command is used to display the type network QoS policy map configuration.

show policy-map type network-qos [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the policy map. If not specified, all type network QoS policy maps will be displayed.
INTERFACE-ID	(Optional) Specifies the module and port number.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the class policies configured for the type network QoS policy map. Use the **show policy-map** without specifying the keyword **type network-qos** command to display the class policy configurations of any or all the existing policy maps. Specify the interface with the **interface** keyword to display the type network QoS policy map configuration.

Example

This example shows how to display all of type network QoS policy maps.

```
Switch# show policy-map type network-qos

Type network-qos policy-maps
============================
Policy Map my_policy_map
Class my_class_map
pause


Policy Map my_policy_map_2
Class Map my_class_map_3
```

```
pause

Switch#
```

82. Quality of Service (QoS) Commands

82-1 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** 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.

Command Default Level

Level: 12.

Usage Guideline

This command enters the policy-map class 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 and be policed by a single rate policer.

```
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)# police 1000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#
```

82-2 class-map

This command is used to create or modify a class-map that defines the criteria for packet matching. To remove an existing class map from the switch, use the **no** command to remove an existing class map. The class-map command enters the class-map configuration mode.

class-map [match-all | match-any] *NAME*

no class-map NAME

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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** keyword 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)#
```

82-3 match

This command is used to define the match criteria for a class-map. Use the **no** command to remove the match criteria.

match {access-group name *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [inner]** *VLAN-LIST***}**

no match {access-group name *ACCESS-LIST-NAME* **| cos [inner]** *COS-LIST* **| [ip] dscp** *DSCP-LIST* **| [ip] precedence** *IP-PRECEDENCE-LIST* **| protocol** *PROTOCOL-NAME* **| vlan [inner]** *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. (Optional) **inner** - Specifies to match the inner most CoS of QinQ packets on a Layer 2 class of service (CoS) marking.
[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. (Optional) **ip** - 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. (Optional) **ip** - 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.
inner	(Optional) Specifies to match the inner-most VLAN ID in an 802.1Q double tagged frame.

Default

None.

Command Mode

Class-map Configuration Mode.

Command Default Level

Level: 12.

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)#
```

This example shows how classes called voice and video-n-data are created to classify traffic based on the CoS values. QoS treatment is then given to the appropriate packets in the cos-based-treatment policy map (in this example, the QoS treatment is a single rate policer and a two rate policer for class voice and video-n-data respectively). The service policy configured in this example is attached to Ethernet interface 3.1.

```
Switch# configure terminal
Switch(config)# class-map voice
Switch(config-cmap)# match cos 7
Switch(config-cmap)# exit
Switch(config)# class-map video-n-data
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# police-map cos-based-treatment
Switch(config-pmap)# class voice
Switch(config-pmap-c)# police 8000 1000 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-n-data
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action
set-dscp-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3/0/1
Switch(config-if)# service-policy input cos-based-treatment
Switch(config-if)#
```

82-4 mls qos aggregate-policer

This command is used to define a named aggregate policer for use in policy maps. To delete a named aggregate policer, use the **no** form of this command. The **mls qos aggregate-policer** command is for single rate policing and the **mls qos aggregate-policer cir** command is for two-rate policing.

mls qos aggregate-policer *NAME KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

mls qos aggregate-policer *NAME* **cir** *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

no mls qos aggregate-policer *NAME*

Parameters

NAME	Specifies the name of the aggregate policing rule. The *NAME* parameter can be up to 32 characters, is case sensitive. The policer names must start with an alphabetic character (not a digit) and must be unique across all aggregate policers.
KBPS	Specifies the average rate, in kilobits per second.
BURST-NORMAL	(Optional) Specifies the normal burst size in kilobytes.
BURST-MAX	(Optional) Specifies the maximum burst size, in kilobytes.
CIR	Specifies the committed information rate in Kbps. The committed packet rate is the first token bucket for the two-rate metering.
PIR	Specifies the peak information rate in Kbps. The peak information rate is the second token bucket for the two-rate metering.
CONFORM-BURST	Specifies the burst size for the first token bucket in kilobytes.
PEAK-BURST	Specifies the burst size for the second token bucket in kilobytes.
confirm-action	(optional) Specifies the action to take on green color packets. If the confirm-action is not specified, the default action is transmit.
exceed-action	Specifies the action to take on packets that exceed the rate limit. For two rate policer, if the exceed-action is not specified, the default action is drop.
violation-action	(Optional) Specifies the action to take on packets that violate the normal and maximum burst sizes for singe rate policing. Specifies the action to take for those packets that did not conform to both CIR and PIR. For a single rate policer, If violation-action is not specified, it will create a single rate two color policer. For a two rate policer, if the violation-action is not specified, the default action is equal to the exceed-action.
ACTION	Specifies the action to take on packets. Specify one of the following keywords: **drop** - Drops the packet. **set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. **set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value. **transmit** - Transmits the packet unaltered.

color-aware	(Optional) Specifies the option for the single rate three colors policer or two rates three colors policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in color aware mode.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

An aggregate policer can be shared by different policy map classes in a policy map. It cannot be shared by separate policy maps.

Example

This example shows how an aggregate policer named “agg-policer5” with a single rate two color policer is configured. This named aggregator policer is applied as the service policy for the class 1 and class 2 traffic class in the policy 2 policy map.

```
Switch# configure terminal
Switch(config)# mls qos aggregate-policer agg-policer5 10 1000 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer5
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer5
Switch(config-pmap-c)#
```

82-5 mls qos cos

This command is used to configure the default Class of Service (CoS) value of a port. Use the **no** form of the command to revert the setting to default.

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.

Command Default Level

Level: 12.

Usage Guideline

When the **override** option 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** option is specified, the port default CoS will be applied to all packets received by the port. Use the **override** keyword 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.

For packets arriving at the 802.1Q VLAN tunnel port, the port default CoS will be both the internal CoS assigned to the packet, and the CoS value in the tunnel VLAN tag of the transmitted packet.

Example

This example shows how the default CoS of Ethernet port 3/0/1 is set to 3.

```
Switch# configure terminal
Switch(config)# interface  eth3/0/1
switch(config-if)# mls qos cos 3
switch(config-if)#
```

82-6 mls qos dscp-mutation

This command is used to attach an ingress Differentiated Services Code Point (DSCP) mutation map to the interface. To remove the ingress DSCP mutation map association from the interface, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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 then attach the ingress-DSCP mutation map named “mutemap1” to port eth3/0/1.

```
Switch# configure terminal
Switch(config)# mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)# interface eth3/0/1
Switch(config-if)# mls qos dscp-mutation mutemap1
Switch(config-if)#
```

82-7 mls qos map cos-color

This command is used to define the CoS to color map for mapping a packet’s initial color. To return the map to the default setting, use the **no** form of this command.

mls qos map cos-color *COS-LIST* **to {green | yellow | red}**

no mls qos map cos-color

Parameters

COS-LIST	Specifies the list of CoS values to be mapped to a color. The range of CoS is from 0 to 7. The multiple CoS values in the list can be in the form separated by commas or a range list.

Default

By default, all CoS values are mapped to the green color.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When packets enter the ingress port, they will be colored based on either the DSCP to color map (if the port is a trusted DSCP port) or the CoS to color map (if the port is a trusted CoS port).

Use the **mls qos map cos-color** command, in the interface configuration mode, to configure the CoS to color map. If the ingress port is set to trusted CoS ports, the received packet will be initialized to a color based on this map.

Example

This example shows how to define CoS value 1 to 7 as the red color and 0 as the green color for packets arriving at eth 3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# mls qos map cos-color 1-7 to red
Switch(config-if)#
```

82-8 mls qos map dscp-color

This command is used to define the DSCP to color map for the mapping of a packet's initial color. To return the color map to the default setting, use the **no** form of this command.

mls qos map dscp-color *DSCP-LIST* **to {green | yellow | red}**

no mls qos map dscp-color *DSCP-LIST*

Parameters

dscp *DSCP-LIST*	Specifies the list of DSCP code point to be mapped to a color. The range is from 0 to 63. The multiple DSCP values in the list can be in the form separated by commas or a range list.

Default

There is no mapping. All DSCP code points are mapped to green color.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to define the DSCP to color map for the mapping of a packet's initial color.

Example

This example shows how to define DSCP 61 to 63 as the yellow color and any other IP packet is initialized with the green color at eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# mls qos map dscp-color 61-63 to yellow
Switch(config-if)#
```

82-9 mls qos map dscp-cos

This command is used to define a Differentiated Services Code Point (DSCP)-to-class of service (CoS) map. To return to the default setting, use the **no** form of this command.

mls qos map dscp-cos *DSCP-LIST* **to** *COS-VALUE*

no mls qos map dscp-cos *DSCP-LIST*

Parameters

dscp-cos *DSCP-LIST* **to** *COST-VALUE*	Specifies the list of DSCP code points to be mapped to a CoS 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.
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.

Command Default Level

Level: 12.

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 for eth2/0/6.

```
Switch# configure terminal
Switch(config)# interface eth2/0/6
Switch(config-if)# mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

82-10 mls qos map dscp-mutation

This command is used to define a named Differentiated Services Code Point (DSCP) mutation map. To remove the mutation map, use the **no** form of this command.

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. A series of DSCPs can be separated by commas (,) or hyphens (-). No space or hyphen is 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.

Command Default Level

Level: 12.

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 and DSCP-color 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)#
```

82-11 mls qos scheduler

This command is used to configure the scheduling mechanism. Use the **no** command to reset the packet scheduling mechanism to the default.

mls qos scheduler {sp | rr | wrr | wdrr | ets}

no mls qos scheduler

Parameters

sp	Specifies that all queues are in strict priority scheduling.
rr	Specifies that all queues are in round-robin scheduling.
wrr	Specifies the queues in the frame count weighted round-robin 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 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.

Command Default Level

Level: 12.

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 eth3/0/1
Switch(config-if)# mls qos scheduler sp
Switch(config-if)#
```

82-12 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 the 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.

Command Default Level

Level: 12.

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

When a packet is received by a port, it will be initialized to a color based on the **mls qos map dscp-color** command if the receiving port is to trust DSCP or MLS QoS mapped CoS color if the receiving port is to trust CoS.

Example

This example shows how to configure port eth1/0/1 to trust the DSCP mode.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# mls qos trust dscp
Switch(config-if)#
```

82-13 police

This command is used to configure traffic policing to use the single rate. To remove traffic policing, use the **no** form of this command.

police *KBPS* **[***BURST-NORMAL* **[***BURST-MAX***]] [conform-action** *ACTION***] exceed-action** *ACTION* **[violate-action** *ACTION***] [color-aware]**

no police

Parameters

KBPS	Specifies the average rate, in kilobits per second.
BURST-NORMAL	(Optional) Specifies the normal burst size in kilobytes.
BURST-MAX	(Optional) Specifies the maximum burst size, in kilobytes.
confirm-action	(optional) Specifies the action to take on green color packets. If the action is not specified, the default action is to transmit.
exceed-action	Specifies the action to take on yellow color packets that exceed the rate limit.
violate-action	(Optional) Specifies the action to take on red color packets. When violate-action is not specified, the policer is a single rate two color policer. When violate-action is specified, the policer is a single rate three color policer.

ACTION	Specifies the action to take on packets. Use one of the following keywords: **drop** - Drops the packet. **set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. **set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value. **transmit** - Transmits the packet. The packet is not altered.
color-aware	(Optional) Specifies the option for the single rate three colors policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in the color aware mode.

Default

None.

Command Mode

Policy-map Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **police** command to drop the packet or mark the packet with different quality of service (QoS) values based on conformance level of the packet.

Use the **police** *KBPS* command to create a single rate policer. Use the **police cir** command to create a two rate policer. There are two kinds of single rate policers (1) a single rate two color policer and (2) a single rate three color policer. If the violate action is specified in the **police** *KBPS* command, then the policer is three colors. If not specified, the policer is two colors.

As a packet arrives at a port, the packet will be initialized with a color. If the receive port trusts DSCP then the initial color of the packet is mapped from the incoming DSCP based on the DSCP to color map. If the receipt port trusts CoS then the initial color is mapped from the incoming CoS based on the CoS to color map.

A single rate two color policer can only work in color-blind mode. Both single rate three color policers and two rate three color policers can work in color aware mode. In color-blind mode, the final color of the packet is determined by the policer metering result alone. In color-aware mode, the final color of the packet is determined by the initial color of the packet and the policer metering result. In this case the policer may further downgrade the initial color.

After the policer metering action will be based on the final color. Conform action will be taken on green color packets, exceed-action will be taken on yellow color packets, and violate action will be taken on red color packets. When specifying actions, you cannot specify contradictory actions such as violate-action transmit and exceed-action drop.

The actions configured by the set command for a traffic class will be applied to all the packets belonging to the traffic class.

Example

This example shows how to define a traffic class and associate the policy with the match criteria for the traffic class in a policy map. The **service-policy** command is then used to attach this service policy to the interface. In this particular example, traffic policing is configured with an average rate of 8 kilobits per second and a normal burst size of 1 kilobyte for all ingress packets at eth3/0/1.

```
Switch# configure terminal
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group name acl_rd
```

```
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8 1 exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3/0/1
Switch(config-if)# service-policy input police-setting
Switch(config-if)#
```

82-14 police aggregate

This command is used to configure a named aggregate policer as the policy for a traffic class in a policy map. Use the **no** command to delete the name aggregate policer from a class policy.

police aggregate *NAME*

no police

Parameters

NAME	Specifies a previously defined aggregate policer name as the aggregate policer for a traffic class.

Default

None.

Command Mode

Policy-map Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **mls qos aggregate-policer** command in the global configuration mode to create a named aggregate policer. Then use the **police aggregate** command in the policy-map class configuration mode to configure the named aggregate policer as the policy for a traffic class. A named aggregate policer cannot be referenced from a different policy map. If a named aggregate policer is attached to multiple ingress ports, the metering operation of the policer will not be applied to the aggregate traffic but remains applied to the traffic received on the individual port.

Example

This example shows how to configure a named aggregate policer's parameters and apply the policer to multiple classes in a policy map: An aggregate policer with single rate policing named "agg_policer1" is created. This policer is configured as the policy for traffic class 1, 2, and 3.

```
Switch# configure terminal
Switch(config)# mls qos aggregate-policer agg_policer1 10000 16384 exceed-action drop
Switch(config)# policy-map policy2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police aggregate agg_policer1
```

```
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# police aggregate agg_policer1
Switch(config-pmap-c)#
```

82-15 police cir

This command is used to configure traffic policing for two rates, the committed information rate (CIR) and the peak information rate (PIR). Use the **no** command to remove two-rate traffic policing.

police cir *CIR* **[bc** *CONFORM-BURST***] pir** *PIR* **[be** *PEAK-BURST***] [conform-action** *ACTION***] [exceed-action** *ACTION* **[violate-action** *ACTION***]] [color-aware]**

no police

Parameters

CIR	Specifies the committed information rate in kilobits per second. The committed packet rate is the first token bucket for the two-rate metering.
PIR	Specifies the peak information rate in kilobits per second. The peak information rate is the second token bucket for the two-rate metering.
CONFORM-BURST	(Optional) Specifies the burst size for the first token bucket in kilobytes.
PEAK-BURST	(Optional) Specifies the burst size for the second token bucket in kilobytes.
confirm-action	(Optional) Specifies the action to take on green color packets. If the action is not specified, the default action is transmit.
exceed-action	(Optional) Specifies the action to take for those packets that conform to PIR but not to CIR. These packets are referred to as yellow color traffic. If the exceed-action is not specified, the default action is drop.
violate-action	(Optional) Specifies the action to take for those packets that did not conform to both CIR and PIR. These packets are referred to as red color traffic. If the violate-action is not specified, the default action is equal to the exceed-action.
ACTION	Specifies the action to be taken. The actions can be: **drop** - Packets will be dropped. **set-dscp-transmit** *VALUE* - Sets the IP differentiated services code point (DSCP) value and transmits the packet with the new IP DSCP value. **set-1p-transmit** - Sets the 802.1p value and transmits the packet with the new value. **transmit** - Transmits the packet. The packet is not altered.
color-aware	(Optional) Specifies the option for a two rate three color policer. When color-aware is not specified, the policer works in the color blind mode. When color-aware is specified, the policer works in the color aware mode.

Default

None.

Command Mode

Policy-map Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

As a packet arrives at a port, the packet will be initialized with a color. The receiving port either trusts DSCP or CoS. The initial color of the packet is mapped from the DSCP in the incoming packet if the receiving port trusts DSCP. The initial color of the packet is mapped from the CoS in the incoming packet if the receiving port trusts CoS.

Both single rate three colors policers and two rate three color policers can work in color aware mode. In color-blind mode, the final color of the packet is determined by the policer metering result alone. In color-aware mode, the final color of the packet is determined by the initial color of the packet and the policer metering result; The policer may further downgrade the initial color.

After the policer metering and based on the final color, the conform action will be taken on green color packets, exceed-action will be taken on yellow color packets, and violate action will be taken on red color packets. When specifying the actions, you cannot specify contradictory actions such as violate-action transmit and exceed-action drop.

The actions configured by the set command for the traffic class will be applied to all the packets belonging to the traffic class.

Example

This example shows how two-rate traffic policing is configured on a class called police to limit traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps, and the policy map named policy1 is attached to eth1/0/3.

```
Switch# configure terminal
Switch(config)# class-map police
Switch(config-cmap)# match access-group name myAcl101
Switch(config-cmap)# exit
Switch(config)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth1/0/3
Switch(config-if)# service-policy output policy1
Switch(config-if)#
```

82-16 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. To delete a policy map, use the **no** form of this command.

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.

Command Default Level

Level: 12.

Usage Guideline

Use the **policy-map** 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 access control list (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)#
```

82-17 priority-queue cos-map

This command is used to define a Class of Service (CoS) to queue map. To restore to the default setting, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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)#
```

82-18 queue rate-limit

This command is used to specify or modify the bandwidth allocated for a queue. To remove the bandwidth allocated for a queue, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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 interface eth3/0/1 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 eth3/0/1
Switch(config-if)# queue 1 rate-limit 100 2000
Switch(config-if)# queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

82-19 rate-limit {input | output}

This command is used to set the received bandwidth limit values for an interface. To set the transmit bandwidth limit values on an interface use the **rate-limit output** command in the interface configuration mode. To disable the bandwidth limit, use the **no** form of this command.

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

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 the maximum bandwidth limits are configured on eth2/0/5. The ingress bandwidth is limited to 2000Kbps and 4096K bytes for burst traffic.

```
Switch# configure terminal
Switch(config)# interface eth2/0/5
Switch(config-if)# rate-limit input 2000 4096
Switch(config-if)#
```

82-20 service-policy

This command is used to attach a policy map to an input interface. To remove a service policy from an input interface, use the **no** form of this command.

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 31 alphanumeric characters.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **service-policy** 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 two policy maps are defined: (1) cust1-classes and (2) cust2-classes.

For cust1-classes, gold is configured to match CoS 6 and be policed by a single rate policer with a committed rate of 800 Kbps. Silver is configured to match CoS 5 and be policed by a single rate policer with a committed rate of 2000Kbps, and bronze is configured to match CoS 0 and be policed by a single rate policer with a committed rate of 8000Kbps.

For cust2-classes, gold is configured to use Cos Queue 6 and be policed by a single rate policer with a committed rate of 1600 Kbps. Silver is policed by a single rate policer with a committed rate of 4000 Kbps, and bronze is policed by a single rate policer with a committed rate of 16000 Kbps.

The cust1-classes policy map is configured and then attached to interfaces eth3/0/1 and eth3/0/2 for ingress traffic.

```
Switch# configure terminal
Switch(config)# class-map match-all gold
Switch(config-cmap)# match cos 6
Switch(config-cmap)# exit
Switch(config)# class-map match-all silver
Switch(config-cmap)# match cos 5
Switch(config-cmap)# exit
Switch(config)# class-map match-all bronze
Switch(config-cmap)# match cos 0
Switch(config-cmap)# exit
Switch(config)# policy-map cust1-classes
Switch(config-pmap)# class gold
Switch(config-pmap-c)# police 800000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 2000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 8000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3/0/1
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)# exit
Switch(config)# interface eth3/0/2
Switch(config-if)# service-policy input cust1-classes
Switch(config-if)#
```

The cust2-classes policy map is configured and then attached to interface eth4/0/1 for ingress traffic.

```
Switch# configure terminal
Switch(config)# policy-map cust2-classes
Switch(config-pmap)# class gold
Switch(config-pmap-c)# police 1600000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class silver
Switch(config-pmap-c)# police 4000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# class bronze
Switch(config-pmap-c)# police 16000000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth4/0/1
Switch(config-if)# service-policy input cust2-classes
Switch(config-if)#
```

82-21 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.

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. Setting CoS will not affect the CoS queue selection.
cos-queue *COS-QUEUE*	Specifies to assign the CoS queue to the packets. This overwrites the original CoS queue selection. Setting the CoS queue will not take effect if the policy map is applied for the egress flow on the interface.

Default

None.

Command Mode

Policy-map Class Configuration Mode.

Command Default Level

Level: 12.

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. The user can use the **police** command and the **set** command for the same class. The **set** command will be applied to all colors of packets.

Example

This example shows how the policy map policy1 is configured with the policy for the class1 class. The packets that are included in the class1 class will be set to a DSCP of 10 and policed by a single rate policer with a committed rate of 1Mbps.

```
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)# police 1000000 2000 exceed-action set-dscp-transmit 10
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)#
```

82-22 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 31 alphanumeric characters.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display all class maps and their matching criteria.

Example

This example shows how two class maps are defined. 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#
```

82-23 show mls qos aggregate-policer

This command is used to display the configured aggregated policer.

show mls qos aggregate-policer [*NAME***]**

Parameters

NAME	(Optional) Specifies the name of the aggregate policer.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the configured aggregated policer.

Example

This example shows how to display the aggregate policer.

```
Switch# show mls qos aggregate-policer

mls qos aggregate-policer agg-policer5 10 1000 conform-action transmit exceed-action
drop
mls qos aggregate-policer agg-policer5 cir 500 bc 10 pir 1000 be 10 conform-action
transmit exceed-action set-dscp-transmit 2 violate-action drop

Switch#
```

82-24 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-color | cos-color | dscp-cos}}**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID to display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
cos	Specifies to displays the port default CoS.
scheduler	Specifies to displays the transmit queue scheduling settings.
trust	Specifies to displays the port trust State.
rate-limit	Specifies to displays the bandwidth limitation configured for the port.
queue-rate-limit	Specifies to displays the bandwidth allocation configured for the queue.
dscp-mutation	Specifies to displays the DSCP mutation map attached to the interface.
map dscp-color	Specifies to displays the DSCP to color map.

map cos-color	Specifies to displays the CoS to color map.
map dscp-cos	Specifies to displays the mapping of DSCP to CoS

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display port level QoS configurations.

Example

This example shows how to display the default CoS for eth 1/0/2 to eth 1/0/5.

```
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 eth 1/0/2 to eth 1/0/5.

```
Switch# show mls qos interface eth1/0/2-1/0/5 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 eth1/0/1 to eth1/0/2.

```
Switch# show mls qos interface eth1/0/1-1/0/2 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 eth 1/0/1 to 1/0/2.

```
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 port 1/0/1 to 1/0/4.

```
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 eth 1/0/1 to 1/0/2.

```
Switch# show mls qos interface eth1/0/1-2 queue-rate-limit

eth1/0/1
  QID   Min Bandwidth  Max Bandwidth
  ----  -------------- -------------
  0         -               -
  1         16 kbps         10%(100000 kbps)
  2         32 kbps             -
  3         2%              50%
  4         64 kbps             -
  5         64 kbps             -
  6         32 kbps             -
  7         -               128 kbps
eth1/0/2
  QID   Min Bandwidth  Max Bandwidth
   ----  -------------- -------------
  0         -               -
  1         16 kbps             -
  2         32 kbps             -
  3         32 kbps             -
  4         64 kbps             -
  5         64 kbps             -
  6         32 kbps             -
  7         -               128 kbps

Switch#
```

This example shows how to display the DSCP to color map for port 1/0/1 to port 1/0/2.

```
Switch# show mls qos interface eth1/0/1-2 map dscp-color

eth1/0/1
  DSCP 0–7 are mapped to green
  DSCP 8–40 are mapped to red
  DSCP 41-43 are mapped to yellow
eth1/0/2
  DSCP 0 – 7 are mapped to green

Switch#
```

This example shows how to display the CoS to color map for port 1/0/3 to port 1/0/4.

```
Switch# show mls qos interface eth1/0/3-4 map cos-color

eth1/0/3
  CoS 0,1,2 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red
eth1/0/4
  CoS 0,1-6 are mapped to green

Switch#
```

This example shows how to display the DSCP to CoS map for port 1/0/1.

```
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 01
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#
```

82-25 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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: mutemapl
Attaching interface:
eth1/0/1-10,eth2/0/1-5
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  30 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#
```

82-26 show mls qos queueing

This command is used to display the QoS queuing information and weight configuration for different scheduler algorithm on specified interface(s).

show mls qos queuing [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface ID on which the weight configuration of different scheduler.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

When the optional keyword Interface is entered, the weight configuration for different scheduler (WRR or WDRR) on the specified interface(s) will be displayed. If the interface is not specified, only the system-wide map of CoS to queue ID is 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 queuing information.

```
Switch# show mls qos queueing

Cos-queue map:
CoS UC QID  MC QID
--- ------  ------
0   2       1
1   0       0
2   1       0
3   3       1
4   4       2
5   5       2
6   6       3
7   7       3

Switch#
```

This example shows how to display the weight configuration for the different scheduler on interface eth1/0/3.

```
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#
```

82-27 show policy-map

This command is used to display the policy map configuration.

show policy-map [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Parameters

INTERFACE-ID	(Optional) Specifies the module and port number.
POLICY-NAME	(Optional) Specifies the name of the policy map. If not specified, all policy maps will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

The **show policy-map** command displays the class policies configured for the policy map. Use the **show policy-map** command to display the class policy configurations of any or all the existing service policy maps.

Example

This example shows how in the policy map called policy1, two-rate traffic policing has been configured for the class called police. Two-rate traffic policing has been configured to limit the traffic to an average committed rate of 500 kbps and a peak rate of 1 Mbps.

```
Switch# configure terminal
Switch(config)# class-map police
Switch(config-cmap)# match access-group name acl_rd
Switch(config-cmap)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500 bc 10 pir 1000 be 10 exceed-action set-dscp-
transmit 2 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface eth3/0/1
Router(config-if)# service-policy output policy1
Router(config-if)#
```

This example shows how to the display of the policy map called policy1, created above.

```
Switch# show policy-map policy1

Policy Map policy1
  Class police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop

Switch#
```

This example shows how to display all policy maps at port 3/0/1.

```
Switch# show policy-map interface eth3/0/1

Policy Map: policy1 : input
  Class police
police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-
transmit 2 violate-action drop

Switch#
```

82-28 wdrr-queue bandwidth

This command is used to set the queue quantum in the WDRR scheduling mode. To restore to the default setting, use the **no** form of this command.

wdrr-queue bandwidth *QUANTUM1…QUANTUM127*

no wdrr-queue bandwidth

Parameters

QUANTUM1 …QUANTUM127	Specifies the quantum (frame length count) value of every queue for weighted round-robin scheduling.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The configuration of 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 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 interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# mls qos scheduler wdrr
Switch(config-if)# wdrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

82-29 wrr-queue bandwidth

This command is used to set the queue weight in the WRR scheduling mode. To restore to the default setting, use the **no** form of this command.

wrr-queue bandwidth *WEIGHT1…WEIGHT127*

no wrr-queue bandwidth

Parameters

WEIGHT1 …WEIGHT127	Specifies the weight (frame count) value of every queue for weighted round-robin scheduling.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The configuration of this command takes effect when the scheduling mode is in the WRR mode. Use the **mls qos scheduler wrr** command to change the scheduling mode to WRR mode. To satisfy 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 interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# mls qos scheduler wrr
Switch(config-if)# wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

83. Quantized Congestion Notification (QCN) Commands

83-1 clear qcn counters

This command is used to clear QCN counters.

clear qcn counters {all | interface *INTERFACE-ID* **[, | -] cp** *QID* **[, | -]}**

Parameters

all	Specifies to clear QCN counters on all interfaces.
interface *INTERFACE-ID* **[,	-]**	Specifies the interface to clear QCN counters. Specify multiple interfaces, separated by commas or ranges by using a hyphen. No space before and after the comma or hyphen.
cp *QID* **[,	-]**	Specifies the queue ID (same as the outbound queue ID) to specify which Congestion Point (CP) to clear counters. Specify multiple CPs, separated by commas or ranges by using a hyphen. No space before and after the comma or hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command with the interface keyword to clear QCN counters of CP(s) on the specified interface(s).

Example

This example shows how to reset QCN counters on all interfaces.

```
Switch# clear qcn counters all
Switch#
```

83-2 qcn

This command is used to enable the QCN functionality. Use the **no** form of this command to disable the QCN functionality

qcn enable

no qcn enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

QCN is a form of end-to-end congestion management defined in IEEE 802.1.Qau. The purpose of QCN is to ensure that congestion is controlled from the sending device to the receiving device in a dynamic fashion that can deal with changing bottlenecks. Use this command to enable or disable the QCN functionality.

Example

This example shows how to enable the QCN functionality.

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

83-3 qcn cnm-transmit-priority

This command is used to globally configure the IEEE 802.1p priority for transmitting Congestion Notification Messages (CNMs). Use the **no** form of this command to reset to the default setting.

qcn cnm-transmit-priority *PRIORITY-VALUE*

no qcn cnm-transmit-priority

Parameters

PRIORITY-VALUE	Specifies the IEEE 802.1p priority value for all Congestion Notification Messages (CNMs). The valid priority range of CNMs is from 0 to 7

Default

By default, this value is 6.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the priority of Congestion Notification Messages which are transmitted by the switch.

Example

This example shows how to configure the priority of Congestion Notification Messages to 1.

```
Switch# configure terminal
Switch(config)# qcn cnm-transmit-priority 1
```

```
Switch(config)#
```

83-4 qcn cnpv (global)

This command is used to globally assign IEEE 802.1p priority as Congestion Notification Priority Value (CNPV) and generate per-interface CNPV entries with default settings for all ports. Use the **no** form of this command to delete a priority from CNPV.

qcn cnpv *CNPV-PRIORITY-VALUE* **[cp-creation {auto-enable | auto-disable}]**

qcn cnpv *CNPV-PRIORITY-VALUE* **admin-defense-mode {disable | interior | interior-ready | edge}**

qcn cnpv *CNPV-PRIORITY-VALUE* **alternate-priority** *PRIORITY-VALUE*

qcn cnpv *CNPV-PRIORITY-VALUE* **defense-mode-choice {admin | auto}**

no qcn cnpv *CNPV-PRIORITY-VALUE*

Parameters

CNPV-PRIORITY-VALUE	Specifies the IEEE 802.1p priority value to be the Congestion Notification Priority Value (CNPV). The valid priority range of CNPV is from 0 to 7.
cp-creation	(Optional) Specifies that when assigning a priority as the CNPV, you can specify the default value for the defense mode choice of newly-created port entries. **auto-enable** - Takes *comp* as the defense mode choice for newly-created port entries, that is the defense mode and alternate priority are determined by the global setting. **auto-disable** - Takes *admin* as the defense mode choice for newly-created port entries, that is the defense mode and alternate priority are determined by the per-port administrator's setting. If not specified, the default **cp-creation** is **auto-enable**.
admin-defense-mode	(Optional) Specifies the default CND defense mode for this CNPV on all interfaces. This setting can be overridden by the **admin-defense-mode** of per-interface. **disable** - The congestion notification capability is administratively disabled for this priority. **interior** - The priority parameter of frame input are not remapped to or from this priority and the frames are transmitted without a CN-TAG. **interior-ready** - The priority parameter of frame input is not remapped to or from this priority and the CN-TAGs won't be stripped when transmitting the frames. **edge** - The priority parameter of frame input at this priority is remapped to an alternate value. Frames at other priorities are not remapped to this priority and the frames are transmitted without a CN-TAG. If not specified, the default administrative defense mode is **interior**.
alternate-priority *PRIORITY-VALUE*	(Optional) Specifies a priority value to which this priority value is to be remapped when the receiving frame with a Dot1p priority equal to the specified CNPV at Edge port. The valid priority range is from 0 to 7. This value can be overridden by the **alternate-priority** option of the per-interface command. If not specified, the default alternate priority is 0.

defense-mode-choice	(Optional) Specifies how to choose CND defense mode and alternate priority for this CNPV on all ports. This setting can be overridden by **defense-mode-choice** option of the per-interface command. **admin** - The default CND defense mode and alternate priority are specified by administrator. **auto** - The default CND defense mode and alternate priority are controlled automatically. If not specified, the default defense mode choice is **auto**.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the priority to be the Congestion Notification Priority Value (CNPV) and configure the setting for this CNPV. When an IEEE 802.1p priority is assigned as a CNPV globally, the CNPV configuration for all interfaces will be created with a default value. When a priority is deleted from CNPV, the CNPV configuration for all interfaces will be deleted.

Example

This example shows how to assign the CoS priority 3 to CoS queue 2. Assign priority 3 as the CNPV and take **admin** as the defense mode choice for newly created port entries.

```
Switch# configure terminal
Switch(config)# priority-queue cos-map 2 3
Switch(config)# qcn cnpv 3 cp-creation auto-disable
Switch(config)#
```

This example shows how to configure the priority 2 as the CNPV and administratively assign the defense mode for all ports as **Edge**. Moreover, it assigns the default alternate priority to 1 for all ports.

```
Switch# configure terminal
Switch(config)# qcn cnpv 2 defense-mode-choice admin
Switch(config)# qcn cnpv 2 admin-defense-mode edge
Switch(config)# qcn cnpv 2 alternate-priority 1
Switch(config)#
```

83-5 qcn cnpv (interface)

This command is used to configure the QCN settings in the interface configuration mode.

qcn cnpv *CNPV-PRIORITY-VALUE* **admin-defense-mode {disable | interior | interior-ready | edge}**

qcn cnpv *CNPV-PRIORITY-VALUE* **alternate-priority** *PRIORITY-VALUE*

qcn cnpv *CNPV-PRIORITY-VALUE* **defense-mode-choice {admin | auto | comp}**

Parameters

CNPV-PRIORITY-VALUE	Specifies the IEEE 802.1p priority value to be the Congestion Notification Priority Value (CNPV). The valid priority range of CNPV is from 0 to 7.
admin-defense-mode	Specifies the CND defense mode for this CNPV on the interface. **disable** - The congestion notification capability is administratively disabled for this priority. **interior** - The priority parameter of frame input are not remapped to or from this priority and the frames are transmitted without a CN-TAG. **interior-ready** - The priority parameter of frame input are not remapped to or from this priority and the CN-TAGs won't be stripped off when transmitting the frames. **edge** - The priority parameter of frame input at this priority are remapped to an alternate value. Frames at other priorities are not remapped to this priority and the frames are transmitted without a CN-TAG. If not specified, the default defense mode is **disable**.
alternate-priority *PRIORITY-VALUE*	Specifies a priority value to which this priority value is to be remapped when the receiving frame with a Dot1p priority is equal to the specified CNPV at the edge port. The valid priority range is from 0 to 7. If not specified, the default alternate priority is 0.
defense-mode-choice	Specifies how the default CND defense mode and alternate priority for this Congestion Notification Priority Value on this interface. **admin** - The default CND defense mode and alternate priority are specified by administrator. **auto** - The default CND defense mode and alternate priority are controlled automatically. **comp** - The default CND defense mode and alternate priority are determined by global setting. If not specified, the default defense mode choice is **comp**.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the global **qcn cnpv** command to assign the priority value as a CNPV first. When you issue the command in the interface configuration mode and specify a priority which has not been globally assigned as a CNPV an error message will be prompted. The interface CNPV configuration has higher precedence than global CNPV configuration. That means the modification of the interface CNPV configuration overrides the global CNPV configuration.

The rule to determine the defense mode and alternate priority for a CNPV is specified in the following table.

defense-mode-choice (interface)	defense-mode-choice (global)	Defense mode selected by	Alternate priority is selected by
admin	any	**admin-defense-mode** (interface)	**alternate-priority** (interface)
auto	any	Controlled by the LLDP	Controlled automatically (*).

		Congestion Notification TLV.	
comp	**admin**	**admin-defense-mode** (global)	**alternate-priority** (global)
comp	**auto**	Controlled by the LLDP Congestion Notification TLV.	Controlled automatically (*).

(*) The rule to automatically determine the alternate priority: An integer indicating the next lower priority value than this CNPV that is not a CNPV in an end station or bridge component, or the next higher non-CNPV, if all lower values are CNPVs.

For example, to administratively deactivate the CNPV on the specified interface:

- Use the **qcn cnpv interface configuration** command with the optional keyword **defense-mode-choice** to set the defense mode choice to admin.
- Use the optional keyword **admin-defense-mode** with the argument **disable**.

When a queue ID is used for a CNPV the switch will attach a Congestion Point (CP) on the corresponding outbound queue for each port. When you set the defense mode to disabled for a CNPV on an interface, it probably causes the congestion detection at the corresponding outbound queue on this interface be disabled. In other words, the switch will disable the interface's corresponding CP function when this interface has no active (non-disabled) CNPV mapped to that queue ID. For example, if a CNPV is only enabled on a single interface and no other active (non-disabled) CNPVs use the same queue ID, it implies the corresponding CPs on other egress ports are inactive then no CNMs can be triggered for the incoming traffic from this single enabled interface. To make the Congestion Notification Domain (CND) work correctly you need enable a CNPV on more than one interface.

The command only takes effect when the QCN is enabled globally.

Example

This example shows how to administratively assign the defense mode to interior for CNPV 2 at interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# qcn cnpv 2 defense-mode-choice admin
Switch(config-if)# qcn cnpv 2 admin-defense-mode interior
Switch(config-if)#
```

83-6 qcn cp

This command is used to configure the settings of the Congestion Point (CP).

qcn cp *CP-QID* **{set-point** *QSP-VALUE* **| weight** *WEIGHT-VALUE* **| sample-base** *SAMPLE-BASE-VALUE* **| min-header-octets** *MIN-HEADER-VALUE***}**

Parameters

CP-QID	Specifies the queue ID that the Congestion Point (CP) is attached to. The relation between the queue ID and CP is one-to-one. The CP is specified by the queue ID to which the CP is attached to.
set-point *QSP-VALUE*	Specifies the set point (*cpQSp*) in octets for the queue managed by this CP. Congestion Notification Messages are transmitted to the sources of the frames queued in this CP's queue in order to keep the

	total number of octets stored in the queue at this set point. The valid set point range is from 100 to 4294967295.
weight *CPWEIGHT-VALUE*	Specifies the weight change in the queue length in the calculation of the *cpFb* which is used to determine the value of the Quantized Feedback. The weight *cpW* is equal to two to the power of this value. Thus, setting the variable to -1, means the *cpW* is equal to a half. The valid weight range is from -10 to 10.
sample-base *SAMPLEBASE-VALUE*	Specifies the minimum number of octets to queue in the CP's queue between transmissions of CNMs. The valid sample base range is from 10000 to 4294967295.
min-header-octets *MIN-HEADER-VALUE*	Specifies the minimum number of octets to be returned in a CNM from the data frame that triggered transmission of the CNM. The valid range is from 0 to 64.

Default

The default set point for the queue is 26000 octets.

The default feedback weight is 2 to the power of 1.

The default sample base is 15000 octets.

The default minimum header size is 0.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When a priority is assigned as a CNPV by the **qcn cnpv** global configuration mode command the switch will attach a CP on the corresponding outbound queue for each port. Which queue the CP is attached to depends on CoS mapping. Because the relation between the queue ID and CP is one-to-one, the CP is specified by the queue ID to which the CP is attached to. Use the **qcn cp** command to configure the parameters for the CP.

Specify a queue ID on which no CP is attached. If the queue is not used by any CNPV, the configuration won't take effect.

The CP monitors the transmission queue at the egress port. When you set the defense mode to disabled for a CNPV on an interface and no other active (non-disabled) CNPVs uses the same queue ID, the corresponding CP on that interface will be disabled. That is no CNM can be triggered at this outbound queue.

Use this command to configure the set point (*cpQSp*) and weight (*cpW*) which play roles in the calculation of the *cpFb* which is used to determine the value of the Quantized Feedback. The Quantized Feedback (6-bit) is a field of a CNM and indicates the degree of congestion.

In other words, the *cpFb* has two terms. The first term is the difference between the current and the desired queue lengths. The second is a weight factor *cpW* times the difference between the current and the previous queue lengths (*cpQDelta*). Thus, a multiple of the first derivative of the queue size is subtracted from the current non-optimality of the queue, so that if the queue length is moving toward the set point *cpQSp*, the *cpFb* will be closer to 0 than if the queue length is moving away from the *cpQSp*.

Use this command to configure the CP's settings in the interface configuration mode.

This command only takes effect when the QCN is enabled globally.

Example

This example shows how to configure the CP for interface eth1/0/1.

```
Switch# configure terminal
```

```
Switch(config)# interface eth1/0/1
Switch(config-if)# qcn cp 1 set-point 30000
Switch(config-if)# qcn cp 1 weight 1
Switch(config-if)# qcn cp 1 sample-base 160000
Switch(config-if)# qcn cp 1 min-header-octets 10
Switch(config-if)#
```

83-7 show qcn cnpv

This command is used to display the QCN CNPV settings and status.

show qcn cnpv [status]

Parameters

status	(Optional) Specifies to display the total discarded frames, auto-alternate priority, and error port list for the CNPV.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the configured QCN CNPV configuration.

Example

This example shows how to display the QCN CNPV settings.

```
Switch# show qcn cnpv

Dot1p             Defense     Admin          Alternate Auto Alt. CP
Priority Queue ID Mode Choice Defense Mode   Priority  Priority  Creation
-------- -------- ----------- -------------- --------- --------- -----------
   1        3      admin       interior           0         0     enable
   2        4      auto        interior-ready     0         0     disable

Switch#
```

This example shows how to display the total discarded frames, auto-alternate priority, and error port list for all CNPVs.

```
Switch# show qcn cnpv status

QCN Status             : Enabled
QCN Discarded Frames   : 1234
CNM Transmit Priority  : 1
CNPV: 1
```

```
------------------------------

Auto Alternate Priority : 0
Errored Portlist        : ---

CNPV: 2
------------------------------
Auto Alternate Priority : 0

Errored Portlist        : ---
!---Output Suppressed.

Switch#
```

83-8 show qcn cnpv interface

This command is used to display the QCN configuration and status for each CNPV.

show qcn cnpv *PRIORITY-VALUE* **[, | -] interface [***INTERFACE-ID* **[, | -]] [simple]**

Parameters

PRIORITY-VALUE **[, | -]**	Specifies the priority value to display. The valid priority value range is from 0 to 7. Specify multiple priority values, separated by commas or ranges by using a hyphen. No space before and after the comma or hyphen.
INTERFACE-ID **[, | -]**	(Optional) Specifies the interface to display QCN CNPV information. Specify multiple interfaces, separated by commas or ranges by using a hyphen. No space before and after the comma or hyphen.
simple	(Optional) Specifies to only display the CND defense mode which would operate for the CNPV as determined by the LLDP Congestion Notification TLV.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the QCN configuration and status for each CNPV.

Example

This example shows how to display the QCN configuration on all interfaces for CNPV 1.

```
Switch# show qcn cnpv 1 interface

CNPV: 1
Intf.    Defense     Admin          Auto           Alt. Defense Mode   Alt. Pri.
```

```
Id       Mode Choice Defense Mode   Defense Mode   Pri. (active)       (active)
-------- ----------- -------------- -------------- ---- -------------- ---------
eEth1/0/1 comp        interior-ready N/A              0   interior-ready     0
eEth1/0/2 comp        edge           N/A              0   interior-ready     0
eEth1/0/3 admin       edge           N/A              0   edge               0
eEth1/0/4 comp        interior       N/A              0   interior-ready     0
eEth1/0/5 auto        edge           interior         0   interior           0
eEth1/0/6 comp        edge           N/A              0   interior-ready     0
eEth1/0/7 comp        edge           N/A              0   interior-ready     0
eEth1/0/8 comp        edge           N/A              0   interior-ready     0
eEth1/0/9 comp        edge           N/A              0   interior-ready     0
!--- Output suppressed.

Switch#
```

This example shows how to display the QCN configuration for CNPV 1 on interface, eth1/0/1.

```
Switch# show qcn cnpv 1 interface eth1/0/1

CNPV                        : 1
Interface Id                : eth1/0/1
Defense Mode Choice         : comp
Admin Defense Mode          : interior-ready
Auto Defense Mode           : -----
Alternate Priority          : 0
Defense Mode (active)       : interior-ready
Alternate Priority (active) : 0
Corresponding CP Queue ID   : 2 (active)

Switch#
```

This example shows how to display the CND defense mode controlled by the LLDP Congestion Notification TLV for all interfaces and CNPV 0 to 7.

```
Switch# show qcn cnpv 0-7 interface simple

Codes:  N/A: Not Applied, I - Interior, IR - Interior Ready, E - Edge

Interface CNPV 0 CNPV 1 CNPV 2 CNPV 3 CNPV 4 CNPV 5 CNPV 6 CNPV 7
--------- ------ ------ ------ ------ ------ ------ ------ ------
eth1/0/1  N/A    I      I      N/A    N/A    N/A    IR     N/A
eth1/0/2  N/A    E      I      N/A    N/A    N/A    IR     N/A
!--- Output suppressed.

Switch#
```

83-9 show qcn cp

This command is used to display the information for the CP.

show qcn cp [counters] {all | interface *INTERFACE-ID* **[, | -] [queue** *QID* **[, | -]]}**

Parameters

counters	(Optional) Specifies only to display CP counters.
all	Specifies to display CP information for all interfaces.
interface *INTERFACE-ID* **[, | -]**	Specifies the interface to display QCN CP information. Specify multiple interfaces, separated by commas or ranges by using a hyphen. No space before and after the comma or hyphen.
queue *QID* **[, | -]**	(Optional) Specifies the queue ID that the CP is attached to. Specify multiple CPs, separated by commas or ranges by using a hyphen. No space before and after the comma or hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the CP information for the specified interface(s).

Example

This example shows how to display CP information for interface eth1/0/1 and with queue ID 1.

```
Switch# show qcn cp interface eth1/0/1 queue 1

Interface Id            : eth1/0/1
CP Index                : 2
Status                  : active
CP Priority             : 0
CP Identifier           : 0011223344550101
MAC Address             : 00:11:22:33:44:55
Queue Set Point         : 26000
Feedback Weight         : 1
Minimum Sample-Base     : 150000
Minimum Header-Octets   : 0

Switch#
```

This example shows how to display CP information for interface eth1/0/1 and with queue ID is 1.

```
Switch# show qcn cp counters interface eth1/0/1 queue 1

Int.    CP  CP
Id        Idx Pri Discarded Frames     Transmitted Frames   Transmitted CNMs
--------  --- --- -------------------- -------------------- --------------------
eth1/0/1  1   0   18446744073709551615 18446744073709551615 18446744073709551615

Switch#
```

83-10 show qcn cpid

This command is used to display the relationship between the CP identifier, interface, and CP index.

show qcn cpid *CP-IDENTIFIER*

Parameters

CP-IDENTIFIER	Specifies the 16 hexadecimal digits for the Congestion Point Identifier (CPID) to get the corresponding interface ID and CP index.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the corresponding interface ID and CP index for the specified CP Identifier. This CP index is an arbitrary integer indexing the entries in the CP table among the entries for the same interface. This value is the corresponding queue ID plus 1.

Example

This example shows how to display the interface ID and CP index for CP identifier, 0011223344550101.

```
Switch# show qcn cpid 0011223344550101

CP-Identifier           : 0011223344550101
QCN Component Id        : 1
Interface Index         : eth1/0/1
CP-Index                : 1

Switch#
```

84. Remote Network MONitoring (RMON) Commands

84-1 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.

Command Default Level

Level: 12.

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 Ethernet interface eth3/0/2.

```
Switch# configure terminal
Switch(config)# interface eth3/0/2
Switch(config-if)# rmon collection stats 65 owner guest
Switch(config-if)#
```

84-2 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.

Command Default Level

Level: 12.

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 Ethernet interface 3/0/8.

```
Switch# configure terminal
Switch(config)# interface eth3/0/8
Switch(config-if)# rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

84-3 rmon alarm

This command is used to configure an alarm entry to monitor an interface. To remove an alarm entry, use the **no** form of this command.

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 4294967295.
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 4294967295.
RISING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the ringing 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.

Command Default Level

Level: 12.

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)#
```

84-4 rmon event

This command is used to configure an event entry. To remove an event entry, use the **no** form of this command.

rmon event *INDEX* **[log] [[trap** *COMMUNITY***] [owner** *NAME***] [description** *TEXT***]**

no rmon event *INDEX*

Parameters

INDEX	Specifies the index of the alarm entry. The valid range is from 1 to 65535.
log	Specifies to generate log message for the notification.
trap *COMMUNITY*	Specifies to generate SNMP trap messages for the notification. The maximum length is 127.
owner *NAME*	Specifies the owner string. The maximum length is 127.

description *STRING*	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.

Command Default Level

Level: 12.

Usage Guideline

If the log and not the trap is specified, the created entry will cause a log entry to be generated on an event occurrence. If the trap and not the log is specified, the created entry will cause an SNMP notification to be generated on an event occurrence.

If both the log and trap options 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)#
```

84-5 show rmon alarm

This command is used to displays the alarm configuration.

show rmon alarm

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the RMON alarm table.

Example

This example shows how to displays 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#
```

84-6 show rmon events

This command is used to display the RMON event table.

show rmon events

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the RMON event table.

Example

This example shows how to displays 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, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

84-7 show rmon history

This command is used to display RMON history statistics information.

show rmon history

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays 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 eth4/0/2
  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#
```

84-8 show rmon statistics

This command is used to display RMON Ethernet statistics.

show rmon statistics

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Statistics for all of the configured entries are displayed.

Example

This example shows how to display the RMON statistics.

```
Switch# show rmon statistics

Index 32, owned by it@domain.com, Data Source is  eth4/0/3
  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#
```

84-9 snmp-server enable traps rmon

This command is used to enable the RMON trap state.

snmp-server enable traps rmon [rising-alarm | falling-alarm]

no snmp-server enable traps rmon [rising-alarm | falling-alarm]

Parameters

rising-alarm	Specifies to configure the rising alarm trap state.
falling-alarm	Specifies to configure the falling alarm trap state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables RMON trap state.

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)#
```

85. Route Map Commands

85-1 match interface

This command is used to match the route's outgoing interface.

match interface *INTERFACE-ID*

no match interface

Parameters

INTERFACE-ID	Specifies the outgoing interface.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the route-map configure mode to define rules for matching routes against outgoing interfaces.

Example

This example shows how to create a route map entry to match against the outgoing interface.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match interface vlan1
Switch(config-route-map)#
```

85-2 match ip address

This command is used to match the route based on the IP standard access list.

match ip address {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME***}**

no match ip address {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME***}**

Parameters

ACCESS-LIST-NAME	Specifies a standard or an extended IP access list name.
prefix-list *PREFIX-LIST-NAME*	Specifies an IP prefix list name.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the route map configure mode to define a rule for matching routes against an IP access list.

Example

This example shows how to create an IP access list “myacl” first and create a route map entry to match against the IP access list.

```
Switch# configure terminal
Switch(config)# ip access-list myacl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address myacl
Switch(config-route-map)#
```

85-3 match ip next-hop

This command is used to match the route’s next hop based on the IP standard access list or IP prefix list.

match ip nexthop {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME***}**

no match ip nexthop {*ACCESS-LIST-NAME* **| prefix-list** *PREFIX-LIST-NAME***}**

Parameters

ACCESS-LIST-NAME	Specifies the IP standard access list name.
prefix-list *PREFIX-LIST-NAME*	Specifies an IP prefix list name.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the route map configure mode to define a rule for matching routes against the next hop. The IP address of the next hop will be matched against the IP standard access list or IP prefix list.

Example

This example shows how to create an IP access list “myacl” first and create a route map entry to match against the next hop based on IP access list.

```
Switch# configure terminal
```

```
Switch(config)# ip access-list myacl
Switch(config-ip-acl)# permit  any 10.20.0.0 255.255.0.0
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip next-hop myacl
Switch(config-route-map)#
```

85-4 match ip route-source

This command is used to match the route's source router IP address based on the IP standard access list.

match ip route-source *ACCESS-LIST-NAME*

no match ip route-source

Parameters

ACCESS-LIST-NAME	Specifies a standard IP access list name.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the route map configure mode to define a rule for matching routes against the source router IP address. The IP address of the source router will be matched against the IP standard access list.

Example

This example shows how to create an IP access list "myacl" first and create a route map entry to match against the source router based on the IP access list:

```
Switch# configure terminal
Switch(config)# ip access-list myacl
Switch(config-ip-acl)# permit 10.20.0.0 255.255.0.0 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip route-source myacl
Switch(config-route-map)#
```

85-5 match metric

This command is used to match the route's metric.

match metric *VALUE*

no match metric

Parameters

VALUE	Specifies the metric of route. The range is from 0 to 4294967294.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the route map configure mode to define a rule for matching routes' metric.

Example

This example shows how to create a route map entry to match against the metric of routes.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match metric 10
Switch(config-route-map)#
```

85-6 match route-type

This command is used to match the type of OSPF route.

match route-type {internal | external [type-1 | type-2]}

no match route-type {internal | external [type-1 | type-2]}

Parameters

internal	Specifies the intra-area and inter-area routes of Open Shortest Path First (OSPF).
external	Specifies the autonomous system's external route of OSPF. If the **type-1** and **type-2** options are not specified, **type-1** and **type-2** external routes are included.
type-1	(Optional) Specifies the type-1 external route of OSPF.
type-2	(Optional) Specifies the type-2 external route of OSPF.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the route map configure mode to define a rule for matching type of OSPF routes.

Example

This example shows how to create a route map entry to match against the OSPF internal route.

```
Switch# configure terminal
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match route-type internal
Switch(config-route-map)#
```

85-7 route map

This command is used to create a route map rule entry. Use the **no** form of the command to remove a route map rule entry.

route-map *MAP-NAME* **{permit | deny}** *SEQ-NUMBER*

no route-map *MAP-NAME* **{permit | deny}** *SEQ-NUMBER*

Parameters

MAP-NAME	Specifies the name of the route map.
permit	Specifies that routes that match the rule entry are permitted.
deny	Specifies that routes that match the rule entry are denied.
SEQ-NUMBER	Specifies the sequence number for the route map entry. The value range is from 1 to 65535.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A route map can contain multiple route map entries, which is either a permit entry or a deny entry. When a route is checked against a route map, the entry in the route map will be checked whether match the route based on its sequence number in the route map. If an entry matches, the action associated with the entry will be taken and no further check will be done against the remaining entry in the route map.

A route map entry can contain multiple match and set statements. To match a route against a route map entry, all of the match statements in the route map rule must be satisfied. When a route map entry is matched, all the set statements in the rule will be performed if the entry is a permit entry. The route will be denied if the matched rule is a deny entry.

Example

This example shows how to create a rule entry with the sequence number 1 for route map “myPolicy”.

```
Switch# configure terminal
```

```
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# set community 1:1
Switch(config-route-map)#
```

85-8 show route-map

This command is used to display information about the route map.

show route-map [*ROUTE-MAP-NAME***]**

Parameters

ROUTE-MAP-NAME	(Optional) Specifies the route map to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the route map information.

Example

This example shows how to display the route map information.

```
Switch#show route-map

Route Map map1, permit, sequence 1
  Match clauses:
    ip address PBR_ACL
  Set clauses:
    next-hop 1.0.0.2

Route Map map1, deny, sequence 2
  Match clauses:
    ip address PBR_deny
  Set clauses:
    next-hop 2.0.0.2

Total Entries: 2

Route Map map2, deny, sequence 10
  Match clauses:
    ip address abcde
  Set clauses:
    ip precedence 6

Total Entries: 1
```

```
Total Route Map Counts : 2

Switch#
```

85-9 set ip default next-hop

This command is used to configure the next-hop of routers to route the packets that passes the match clauses of the configured route-map sequences. Use the **no** command to remove specific default next-hops.

set ip default next-hop *IP-ADDRESS* **[…***IP-ADDRESS***]**

no set ip default next-hop *IP-ADDRESS* **[…***IP-ADDRESS***]**

Parameters

IP-ADDRESS	Specifies the IP address for the next-hop or route entry.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used to specify multiple default next hop routers. If default next hops are already configured, the default next hops configured later will be added to the default next hop list. When the first default next hop router specified is down, the next default next hop router specified is tried in turn to route the packet.

Example

This example shows how to configure that PBR will policy route the packets to the next-hop 120.1.2.2 when the source ip is 10.1.1.0/24. The receiving interface is VLAN 100 and cannot find the route in routing table to route the packet. At first, create an IP basic access list, named “Strict-Control” which permits the prefix 10.1.1.0/24. Secondly, create a route map, named “myPolicy” which defines a match rule to associate the IP address prefix-list to the previously created access list, Strict-Control. Lastly, in the VLAN interface configuration mode set the IP policy base route to use the route-map, myPolicy.

```
Switch# configure terminal
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0 0.0.0.255 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set ip default next-hop 120.1.2.2
Switch(config-route-map)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip policy route-map myPolicy
Switch(config-if)#
```

85-10 set ip next-hop

This command is used to configure the next-hop router to route the packet that passes the match clauses of the configured route map sequence. Use the **no** command to remove the clause.

set ip next-hop *IP-ADDRESS* **[…***IP-ADDRESS***]**

no set ip next-hop *IP-ADDRESS* **[…***IP-ADDRESS***]**

Parameters

IP-ADDRESS	Specifies the IP address of the next-hop to route the packet.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used to specify multiple next-hop routers. If next hops are already configured, the next hops configured later will be added to the next hop list. When the first next hop router specified is down, the next next-hop router specified is tried in turn to route the packet.

Example

This example shows how to configure that PBR will policy route the packets to the next-hop 120.1.2.2 when the source IP is 10.1.1.0/24. The receiving interface is VLAN 100. At first, create an IP basic access list, named “Strict-Control” which permits the prefix 10.1.1.0/24. Secondly, create a route map, named “myPolicy” which defines a match rule to associate the IP address prefix-list to the previously created access list, Strict-Control. Lastly, in the VLAN interface configuration mode set the IP policy base route to use the route-map, myPolicy.

```
Switch# configure terminal
Switch(config)# ip access-list Strict-Control
Switch(config-ip-acl)# permit 10.1.1.0 0.0.0.255 any
Switch(config-ip-acl)# exit
Switch(config)# route-map myPolicy permit 1
Switch(config-route-map)# match ip address Strict-Control
Switch(config-route-map)# set ip next-hop 120.1.2.2
Switch(config-route-map)# exit
Switch(config)# interface vlan100
Switch(config-if)# ip policy route-map myPolicy
Switch(config-if)#
```

85-11 set ip precedence

This command is used to configure the precedence value in the IP header. Use the **no** form of the command to remove the setting.

set ip precedence {*NUMBER* **|** *NAME***}**

no set ip precedence

Parameters

NUMBER	Specifies the number of the precedence value to use in the IP header. The following numbers represent the following names: • 0 - Routine. • 1 - Priority. • 2 - Immediate. • 3 - Flash. • 4 - Flash-override. • 5 - Critical. • 6 - Internet. • 7 - Network.
NAME	Specifies the name of the precedence value to use in the IP header.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to set the precedence value in the IP header. This command only takes effect when policy routing involves the IPv4 packet. The precedence can be set using either a number or the corresponding name.

Example

This example shows how to configure the IP precedence value to 5 (critical) for packets that pass the route map match.

```
Switch# configure terminal
Switch(config)# route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set ip precedence 5
Switch(config-route-map)#
```

85-12 set metric

This command is used to modify the metric of routes. Use the **no** form of this command to revert this value back to the default value.

set metric *VALUE*

no set metric

Parameters

VALUE	Specifies the metric of route. The range is from 0 to 4294967294.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to modify the metric of routes.

Example

This example shows how to configure the metric of routes that pass the route map match to 100.

```
Switch# configure terminal
Switch(config)# route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set metric 100
Switch(config-route-map)#
```

85-13 set metric-type

This command is used to configure the type of OSPF AS external route.

set metric-type {type-1 | type-2}

no set metric-type

Parameters

type-1	Specifies to use the OSPF external type-1 metric.
type-2	Specifies to use the OSPF external type-2 metric.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to set the type of OSPF AS external route.

Example

This example shows how to configure the route type to type-2 for the OSPF AS external routes that pass the route map match.

```
Switch# configure terminal
Switch(config)# route-map example permit 10
Switch(config-route-map)# match ip address IPACL_01
Switch(config-route-map)# set metric-type type-2
Switch(config-route-map)#
```

86. Router Advertisement (RA) Guard Commands

86-1 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. Use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an RA guard policy. This command will enter into 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)#
```

86-2 device-role

This command is used to configure the role of the attached device. Use the **no** form of the command to reset 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used to set the role of the attached device. By default, the device role is **host**, and therefore 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)#
```

86-3 match ipv6 access-list

This command is used to filter the RA messages based on the sender IPv6 address. Use the **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

86-4 ipv6 nd raguard attach-policy

This command is used to apply an RA guard policy on a specified interface. Use the **no** command to remove the binding.

ipv6 nd raguard attach-policy [*POLICY-NAME***]**

no ipv6 nd raguard

Parameters

POLICY-NAME	(Optional) Specifies the IPv6 RA guard policy name.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only one RA policy can be attached. If the policy name is not specified, the default policy will set the device role to **host**.

Example

This example shows how to apply the RA guard policy on interface eth1/0/3.

```
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)#
```

86-5 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) Specifies the IPv6 RA guard policy name.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the policy name is specified, only the specified policy information is displayed. If the policy name is not specified, information is displayed for all policies.

Example

This example shows how to display the policy configuration for a policy named “raguard1” and all the interfaces where the policy is applied.

```
Switch# show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
      Device Role: host
      Target: eth1/0/1-1/0/2

Switch#
```

87. Routing Information Protocol (RIP) Commands

87-1 distance (RIP)

This command is used to define an administrative distance of routes learned by IPv4 routing protocols. Use the **no** command to restore the default setting.

distance *DISTANCE*

no distance

Parameters

DISTANCE	Specifies the administrative distance. The range is from 10 to 255. The lower value represents a better route. The value of 0 to 9 is reserved for special use.

Default

By default, the RIP distance is 100.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the distance is an integer from 1 to 999 representing the trust rating of the route. The route with lower distance value is preferred over the route with the higher distance value. Routes with the distance 255 will not be installed for the routing of packets since it indicates that the route is not trusted.

Example

This example shows how to configure the distance of RIP routes to 100.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-rtr)# distance 100
Switch(config-rtr)#
```

87-2 address-family (RIP)

This command is used to enter the address family configuration mode to configure the setting specific to the address family. Use the **no** form of command to revert the setting of the specified address family to the default.

address-family ipv4 vrf *VRF-NAME*

no address-family ipv4 vrf *VRF-NAME*

Parameters

vrf *VRF-NAME*	Specifies the name of the VRF instance to enter VRF address family configuration mode.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the address family configuration mode to configure the command. Use the **exit** command to leave address family configuration mode and return to router configuration mode without removing the existing configuration.

Example

This example shows how to enter and exit address family configuration mode for the VRF “branch-route” address family.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf branch-route
Switch(config-router-af)# exit
Switch(config-router)#
```

87-3 default-metric (RIP)

This command is used to configure the value to be used as the default metric for routes redistributed to RIP. To return to the default value, use the **no** form of the command.

default-metric *METRIC-VALUE*

no default-metric

Parameters

METRIC-VALUE	Specifies the default metric value. The valid range of values is from 1 to 16.

Default

By default, this value is 1.

Command Mode

Router Configuration Mode.

Router Address Family Configuration (RIP) Mode.

Command Default Level

Level: 12.

Usage Guideline

The default metric is used in redistributing routes from other routing protocols. The routes being redistributed are learned by other protocols and have incompatible metric as RIP. The specifying of the metric allows the metric to be synced.

Example

This example shows how to configure the default metric 5 for redistribute the OSPF routes. In other words, assigns the OSPF-derived routes a RIP metric of 5.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# default-metric 5
Switch(config-router)# redistribute ospf
Switch(config-router)#
```

87-4 ip rip authentication text-password

This command is used to enable authentication for RIP version 2 packets and to specify the key that can be used on an interface. To disable authentication, use the **no** form of this command.

ip rip authentication text-password *PASSWORD*

no ip rip authentication text-password

Parameters

PASSWORD	Specifies a password string.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable authentication for RIP version 2 packets and to specify the key that can be used on an interface.

Example

This example shows how to configure authentication on interface VLAN 3.

```
Switch# configure terminal
Switch(config)# interface vlan3
Switch(config-if)# ip rip authentication mode text
Switch(config-if)# ip rip authentication text-password test1
Switch(config-if)#
```

87-5 ip rip authentication mode

This command is used to specify the type of authentication used in RIP version 2 packets. Use the **no** command to revert to the default setting.

ip rip authentication mode text

no ip rip authentication mode

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

RIP version 1 does not support authentication. This command only takes effect for RIP version 2.

Example

This example shows how to enable the authentication at interface VLAN 2.

```
Switch# configure terminal
Switch(config)# interface vlan2
Switch(config-if)# ip rip authentication mode text
Switch(config-if)#
```

87-6 ip rip receive version

This command is used to specify a RIP version to receive on an interface basis. Use the **no** form of the command to revert to the default setting.

ip rip receive version [1] [2]

no ip rip receive version

Parameters

1	(Optional) Specifies to accept RIP version 1 packets.
2	(Optional) Specifies to accept RIP version 2 packets.

Default

By default, the global setting will be used.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the version of the receive RIP version for an interface. If not specified, the global setting is followed.

Example

This example shows how to configure the interface (VLAN 1) to accept both RIP version 1 and version 2 packets.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ip rip receive version 1 2
Switch(config-if)#
```

87-7 ip rip send version

This command is used to specify a RIP version to send on an interface basis. Use the **no** form of the command to revert to the default setting.

ip rip send version [1 | 2]

no ip rip send version

Parameters

1	(Optional) Specifies to send RIP version 1 packets.
2	(Optional) Specifies to send RIP version 2 packets.

Default

By default, the global setting will be used.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the send RIP version for an interface. If not specified, the global setting is followed.

Example

This example shows how to configure the interface VLAN 100 to send RIP version 1 packets.

```
Switch# configure terminal
Switch(config)# interface vlan100
Switch(config-if)# ip rip send version 1
Switch(config-if)#
```

87-8 ip rip v2-broadcast

This command is used to enable the sending of version 2 RIP update packets as broadcast packets instead of multicast packets. Use the **no** form of command to revert to the default setting.

ip rip v2-broadcast

no ip rip v2-broadcast

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

RIP version 2 improves version 1 by sending multicast packets instead of broadcast packets in order to reduce the load on unnecessary hosts on the LAN to process the broadcast packet.

Use this command to broadcast RIP version 2 updates to devices that do not listen to multicast packets. If enabled, version 2 packets will be sent to the IP broadcast address instead of the IP multicast address 224.0.0.9.

Example

This example shows how to configure the interface VLAN 100 to broadcast version 2 RIP packets.

```
Switch# configure terminal
Switch(config)# interface  vlan100
Switch(config-if)# ip rip send version 2
Switch(config-if)# ip rip v2-broadcast
Switch(config-if)#
```

87-9 network

This command is used to specify a network as one that runs RIP. To remove an entry, use the **no** form of this command.

network *NETWORK-PREFIX*

no network *NETWORK-PREFIX*

Parameters

NETWORK-PREFIX	Specifies the subnet prefix of the network.

Default

None.

Command Mode

Router Configuration Mode.

Router Address Family Configuration (RIP) Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify networks in which routing updates will be sent and received. The interface that has a subnet defined belonging to a network specified by this command will be activated with RIP.

Example

This example shows how to define RIP as the routing protocol to be used on all interfaces connected to networks 192.168.70.0/24 and network 10.99.0.0/16.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# network 192.168.70.0
Switch(config-router)# network 10.99.0.0
Switch(config-router)#
```

87-10 passive-interface

This command is used to disable the sending and receiving of routing updates on an interface. Use the **no** form of this command to revert to the default setting.

passive-interface {default | *INTERFACR-ID***}**

no passive-interface {default | *INTERFACR-ID***}**

Parameters

default	Specifies the global default passive state for interfaces.
INTERFACR-ID	Specifies the interface identifier for setting the passive state. If passive state of an interface is not specified, it follows the global default passive state.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If you disable the sending and receiving of routing updates on an interface, the router will not send and receive multicast RIP packets out through the interface, however, the RIP packet from other routers received on this interface continue to be processed.

Example

This example shows how to disable the sending and receiving of routing updates on the interface VLAN 1.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# passive-interface vlan1
Switch(config-router)#
```

87-11 redistribute (RIP)

This command is used to redistribute routes from other routing domains into RIP. Use the **no** command to disable route redistribution from a specific protocol.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE*] **[route-map** *MAP-NAME*]

no redistribute *PROTOCOL* **[metric] [route-map]**

Parameters

PROTOCOL	Specifies the protocol whose routes are to be redistributed. The **static** keyword means to redistribute IP static routes. The **connected** keyword refers to routes that are established automatically by virtue of configuring IP address on an interface.
metric *METRIC-VALUE*	(Optional) Specifies the value to be used as metric for the redistributed routes. The range is from 0 to 16.
route-map *MAP-NAME*	(Optional) Specifies the route map that is used in the filtering of the routes to be redistributed to the current routing protocol. If not specified, all routes are redistributed.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Router Address Family Configuration (RIP) Mode.

Command Default Level

Level: 12.

Usage Guideline

If the metric option is not specified or is specified as 0, the following rules are applied:

- The metric of the redistributed static route or connected route will be 1, if the metric option is not specified, or is specified as 0.
- The metric of the redistributed route from other protocols to the RIP process will be determined by the default metric command if the metric option is not specified.
- The metric of the redistributed route from other protocols to RIP process will be 1 if the metric option is specified as 0.

If the default metric is not specified, then the original metric from the redistributed protocol will be transparently carried through.

If a route map is configured but the route map doesn't exist, it means all routes are not permitted. If a route map sequence has no match entry defined, then all routes will match this sequence.

Example

This example shows how to configure that the specified OSPF process routes will be redistributed into an RIP domain. The OSP-derived metric will be remapped to 10.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# redistribute ospf  metric 10
```

```
Switch(config-router)#
```

87-12 router rip

This command is used to configure the RIP routing process. To disable the RIP routing process, use the **no** form of this command.

router rip

no router rip

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enter the Router Configuration Mode of the RIP protocol and enable the RIP function. The **no** command will remove the configuration in the RIP router mode and disable RIP process.

Example

This example shows how to begin the RIP routing process.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)#
```

87-13 show ip rip database

This command is used to display the Routing Information Protocol (RIP) routing database.

show ip rip database [*IP-ADDRESS MASK* **|** *NETWORK-PREFIXIPREFIX–LENGTH***] [vrf** *VRF-NAME***]**

Parameters

IP-ADDRESS MASK	(Optional) Specifies the address of the routing information that should be displayed.
NETWORK-PREFIXIPREFIX-LENGTH	Specifies the subnet prefix and the prefix length of the network to be displayed.
vrf *VRF-NAME*	(Optional) Specifies to display the routing information in the VRF instance.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Summary address entries will appear in the database only if relevant child routes exist and are being summarized. When the last child route for a summary address becomes invalid, the summary address is also removed from the routing table.

Example

This example shows how to display a summary address.

```
Switch# Show ip rip database

Codes: R - RIP, Rc - RIP connected, K - Kernel,
       C – Connected, S – Static, O – OSPF, B – BGP, A – Aggregate
   Network            Next Hop   Metric  From            If     Time
Rc 10.1.0.0/16                       1                 vlan1
Rc 20.0.0.0/8                        1                 vlan2
R  30.0.0.0/8         20.33.24.1     2  20.33.24.1     vlan2  0DT0H2M44S
                      40.33.24.8     5  40.33.24.2     vlan3  0DT0H2M30S
RA 10.0.0.0/8                        2                        0DT0H0M59S

Total Entries: 4 entries, 5 routes

Switch#
```

87-14 show ip rip interface

This command is used to display interface specific information for RIP.

show ip rip interface

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display interface specific information for RIP.

Example

This example shows how to display interface specific information for RIP.

```
Switch# Show ip rip interface

vlan1 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: text
    Passive interface: Disabled
    IP interface address:
      10.72.63.80/8
vlan2 is up, line protocol is up
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: text
    Passive interface: Disabled
    IP interface address:
      20.72.63.80/8
IP summary address:
      11.0.0.0/8

Total Entries: 2

Switch#
```

87-15 timers basic

This command is used to configure the RIP network timers. To restore the default timers use the **no** form of this command.

timers basic *UPDATE INVALID FLUSH*

no timers basic

Parameters

UPDATE	Specifies the update interval in seconds at which the update message is sent. The range is from 1 to 65535.
INVALID	Specifies the invalidate timer in seconds. The range is from 1 to 65535.
FLUSH	Specifies the flush timer in seconds. The range is from 1 to 65535.

Default

The default update time: 30 seconds.

The default invalid time: 180 seconds.

The default flush time: 120 seconds.

Command Mode

Router Configuration Mode.

Router Address Family Configuration (RIP) Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to modify the RIP protocol timers.

Example

This example shows how to configure the RIP timers. Timers of update, invalid, and flush timers are set to 10, 80, and 160 respectively.

```
Switch# configure terminal
Switch(config)# router rip
Switch(config-router)# timers basic 10 80 160
Switch(config-router)#
```

87-16 version

This command is used to specify a RIP version globally as the default version for all interfaces. Use the **no** form of the command to revert to the default setting.

version {1 | 2}

no version

Parameters

1	Specifies to only receive and transmit RIP version 1 packets.
2	Specifies to only receive and transmit RIP version 2 packets.

Default

By default, RIP version 1 and 2 packets are received, but only RIP version 1 packets are sent.

Command Mode

Router Configuration Mode.

Router Address Family Configuration (RIP) Mode.

Command Default Level

Level: 12.

Usage Guideline

This command defines the default RIP version. This version will be overridden if the version is explicitly specified for the interface by using the **ip rip send version** and **ip rip receive version** commands.

Example

This example shows how to configure the RIP version to version 2.

```
Switch# configure terminal
```

```
Switch(config)# router rip
Switch(config-router)# version 2
Switch(config-router)#
```

88. Routing Information Protocol Next Generation (RIPng) Commands

88-1 clear ipv6 rip

This command is used to clear the RIPng process.

clear ipv6 rip

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

When a RIPng process is cleared, the routing database will be cleared and repopulated.

Example

This example shows how to clear the RIPng routing database.

```
Switch# clear ipv6 rip

Clear ipv6 rip? (y/n) [n] y

Switch#
```

88-2 default-metric (RIPng)

This command is used to set the value used as the default metric for routes redistributed to RIPng. To return to the default value, use the **no** form of the command.

default-metric *METRIC-VALUE*

no default-metric

Parameters

METRIC-VALUE	Specifies the default metric value. The valid value is from 1 to 16.

Default

By default, this value is 1.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the default metric for routes redistributed from other routing protocols. If the routes being redistributed are learned from other protocols, then they have an incompatible metric as IPv6 RIP. Re-specifying of metric allows the metric to be synced.

Example

This example shows how to configure the default metric as 5 for the routes redistributed to RIPng.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# default-metric 5
Switch(config-rtr)# redistribute ospf
Switch(config-rtr)#
```

88-3 distance (RIPng)

This command is used to define an administrative distance of routes learned by IPv6 routing protocols. Use the **no** command to restore the default setting.

distance *DISTANCE*

no distance

Parameters

DISTANCE	Specifies the administrative distance. The range is from 1 to 254. The lower value represents better route.

Default

By default, the RIPng distance is 120.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The distance is an integer from 0 to 255 representing the trust rating of the route. The route with a lower distance value is preferred over the route with the higher distance value. A route with a distance of 255 will not be installed for the routing of packets since it indicates that the route is not trusted.

Example

This example shows how to configure the distance of RIPng routes to 100.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# distance 100
```

```
Switch(config-rtr)#
```

88-4 ipv6 rip enable

This command is used to enable an IPv6 RIP routing process on an interface. To disable an IPv6 RIP routing process on an interface, use the **no** form of this command.

ipv6 rip enable

no ipv6 rip enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable IPv6 RIP on required interfaces.

Example

This example shows how to enable the IPv6 RIP routing process on VLAN 1.

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

88-5 ipv6 rip metric-offset

This command is used to set the value to be added to the metric of an IPv6 RIP route received on the configured interface. Use the **no** form of the command to restore the default setting.

ipv6 rip metric-offset *METRIC-VALUE*

no ipv6 rip metric-offset

Parameters

METRIC-VALUE	Specifies the value to be added to the metric of an IPv6 RIP route received on the configured interface. The valid range is from 1 to 16.

Default

By default, this value is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The metric refers to the hop count. By default, when receiving an IPv6 RIP route, a metric value of 1 is added to the route before it is inserted into the routing table. Use this command to influence the metric of routes received on different interface and thus influence the preference of the route.

Example

This example shows how to configure a metric increment of 3 for routes received on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# ipv6 rip metric-offset 3
Switch(config-if)#
```

88-6 ipv6 router rip

This command is used to configure the IPv6 RIP routing process. To remove an IPv6 RIP routing process, use the **no** form of this command.

ipv6 router rip

no ipv6 router rip

Parameters

None.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enter the Router Configuration Mode for IPv6 RIP routing process. Use the **no** form of the command to remove an IPv6 RIP routing process.

Example

This example shows how to configure an IPv6 RIP routing process.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)#
```

88-7 poison-reverse

This command is used to enable the poison reverse processing for an IPv6 RIP process. Use the **no** form of the command to disable the poison-reverse processing.

poison-reverse

no poison-reverse

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the poison reverse command to enable the poison reverse mechanism in RIP routing updates. When poison reverse is enabled, the routes learned from an interface will be advertised out to the same interface with an unreachable metric.

Example

This example shows how to enable poison reverse for IPv6 RIP.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# poison-reverse
Switch(config-rtr)#
```

88-8 redistribute

This command is used to redistribute routes from other routing domains into RIP. Use the **no** command to disable route redistribution from specific protocols.

redistribute *PROTOCOL* **[metric** *METRIC-VALUE***]**

no redistribute *PROTOCOL*

Parameters

PROTOCOL	Specifies the protocol whose routes are to be redistributed. The **static** keyword means to redistribute IP static routes. The **connected** keyword refers to routes that are established automatically by virtue of configuring IP address on an interface.
metric *METRIC-VALUE*	(Optional) Specifies the value to be used as the metric for the redistributed routes. The range is from 0 to 16.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the metric option is not specified or specified as 0, the following rules are applied:

- The metric of the redistributed static route or connected route will be 1, if the metric option is not specified, or is specified as 0.
- The metric of the redistributed route from other protocols to RIP process will be determined by the default metric command if the metric option is not specified.
- The metric of the redistributed route from other protocols to RIP process will be 1 if the metric option is specified as 0.

If the default metric is not specified, then the original metric from the redistributed protocol will be transparently carried through.

Example

This example shows how to configure the specified OSPF process routes to be redistributed into an RIP domain. The metric will be remapped to 10.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# redistribute ospf  metric 10
Switch(config-rtr)#
```

88-9 show ipv6 rip

This command is used to display interface specific information for RIP.

show ipv6 rip [database]

Parameters

database	(Optional) Specifies to display the entry in the RIP routing database.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the configuration information of RIP protocol.

Use the **show ipv6 rip database** command to display the entry in the RIP routing database.

Example

This example shows how to display the RIP configuration information.

```
Switch# Show ipv6 rip

IPv6 RIP process , port 521, multicast-group FF02::9
Administrative distance is 25.
Maximum paths is 4
     Updates every 60 seconds, expire after 180
     garbage collect after 240
     Split horizon is on; poison reverse is off
     Periodic updates 8883, trigger updates 2
  Interfaces:
    VLAN 100
  Redistribution:
     Redistributing protocol static with metric 10

Switch#
```

88-10 split-horizon

This command is used to enable the split-horizon option for an IPv6 RIP process. Use the **no** form of the command to disable the split-horizon option.

split-horizon

no split-horizon

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable split horizon mechanism in the IPv6 RIP routing update. When split horizon is enabled, the routes learned from an interface will be not advertised out to the same interface.

Example

This example shows how to disable split-horizon for IPv6 RIP.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# no split-horizon
Switch(config-rtr)#
```

88-11 timers

This command is used to configure the IPv6 RIP network timers. To restore the default timers use the **no** form of this command.

timers *UPDATE INVALID FLUSH*

no timers

Parameters

UPDATE	Specifies the update interval at which the update message is sent. The range is from 5 to 65535.
INVALID	Specifies the invalidate timer in seconds. The range is from 1 to 65535.
FLUSH	Specifies the flush timer in seconds. The range is from 1 to 65535.

Default

The default update time: 30 seconds.

The default invalid time: 180 seconds.

The default flush time: 120 seconds.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to modify the IPv6 RIP protocol timers.

Example

This example shows how to configure the RIP timers. The Timers of update, invalid, and flush timers are set to 10, 40, and 160 respectively.

```
Switch# configure terminal
Switch(config)# ipv6 router rip
Switch(config-rtr)# timers 10 40 160
Switch(config-rtr)#
```

88-12 debug ipv6 rip

This command is used to turn on the IPv6 RIP debug function. To turn off the IPv6 RIP debug function, use the **no** form of this command.

debug ipv6 rip

no debug ipv6 rip

Parameters

None.

Default

BY default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the IPv6 RIP debug function while the global debug function has been turned on before.

Example

This example shows how to turn on the IPv6 RIP debug function.

```
Switch# debug ipv6 rip
Switch#
```

88-13 debug ipv6 rip interface

This command is used to turn on the IPv6 RIP interface state debug switch. To turn off the IPv6 RIP interface state debug switch, use the **no** form of this command.

debug ipv6 rip interface

no debug ipv6 rip interface

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the IPv6 RIP interface state debug switch. When the IPv6 RIP interface state changes or some events happen to change the interface state, the debug information will printed if the IPv6 RIP debug function is turned on.

Example

This example shows how to turn on the IPv6 RIP interface state debug switch.

```
Switch# debug ipv6 rip interface
Switch#

The RIPng interface vlan1 has changed the link state to UP
```

88-14 debug ipv6 rip packet-receiving

This command is used to turn on the IPv6 RIP packet receiving debug switch. To turn off the IPv6 RIP packet receiving debug switch, use the **no** form of this command.

debug ipv6 rip packet-receiving

no debug ipv6 rip packet-receiving

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the IPv6 RIP packet receiving debug switch. When one IPv6 RIP protocol packet is received, the debug information will be print if the IPv6 RIP debug function is turned on.

Example

This example shows how to turn on the IPv6 RIP packet receiving debug switch.

```
Switch# debug ipv6 rip packet-receiving
Switch#

Received a RIPng request packet from FE80::1
```

88-15 debug ipv6 rip packet-transmitting

This command is used to turn on the IPv6 RIP packet transmitting debug switch. To turn off the IPv6 RIP packet transmitting debug switch, use the **no** form of this command.

debug ipv6 rip packet-transmitting

no debug ipv6 rip packet-transmitting

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the IPv6 RIP packet transmitting debug switch. When one IPv6 RIP protocol packet is sent out, the debug information will be print if the IPv6 RIP debug function is turned on.

Example

This example shows how to turn on the IPv6 RIP packet transmitting debug switch.

```
Switch# debug ipv6 rip packet-transmitting
Switch#

Send a RIPng response packet to FE80::1 , Index 1
```

88-16 debug ipv6 rip route

This command is used to turn on the IPv6 RIP route debug switch. To turn off the IPv6 RIP route debug switch, use the **no** form of this command.

debug ipv6 rip route

no debug ipv6 rip route

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to turn on or turn off the IPv6 RIP route debug switch. When one IPv6 RIP route is added, updated or deleted, the debug information will be print if the IPv6 RIP debug function is turned on.

Example

This example shows how to turn on the IPv6 RIP route debug switch.

```
Switch# debug ipv6 rip route
Switch#

Add a Static route to RIPng route table dst= 2000::1 nexthop= FE80::1
```

89. Safeguard Engine Commands

89-1 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If this command is issued without parameters, then all CPU protect related counters will be cleared.

Example

This example shows how to clear all CPU protect related statistics.

```
Switch# clear cpu-protect counters all
Switch#
```

89-2 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	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	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.

Command Default Level

Level: 12.

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)#
```

89-3 cpu-protect sub-interface

This command is used to configure the rate limit for traffic destined to the CPU by sub-interface types.

cpu-protect sub-interface {manage | protocol | route} pps *RATE*

no cpu-protect sub-interface {manage | protocol | route}

Parameters

sub-interface [manage | protocol | route]	Specifies the sub-interface type. If no sub-interface is specified then all sub-interfaces will be configured.
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.

Command Default Level

Level: 12.

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)#
```

89-4 cpu-protect type

This command is used to configure the rate limit of traffic destined to the CPU by the protocol type.

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.

Command Default Level

Level: 12.

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
bgp	Border Gateway Protocol	Protocol
dhcp	Dynamic Host Configuration	Protocol
dns	Domain Name Services	Protocol
dvmrp	Distance Vector Multicast Routing Protocol	Protocol
gGvrp	GARP VLAN Registration Protocol	Protocol
icmp	IPv4 Internet Control Message Protocol	Protocol
icmpv6-ndp	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
ntp	Network Time Protocol	Protocol
ospf	Open Shortest Path First	Protocol
pim	Protocol Independent Multicast	Protocol
pppoe	Point-to-Point Protocol over Ethernet	Protocol
rip	Routing Information 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
vrrp	Virtual Router Redundancy Protocol	Protocol
web	HTTP and HTTPS	Manage

Example

This example shows how to configure the threshold of OSPF protocol packets as 100 packets per second.

```
Switch# configure terminal
Switch(config)# cpu-protect type ospf pps 100
Switch(config)#
```

89-5 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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         : 50%
    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.

89-6 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} [*UNIT-ID***]**

Parameters

UNIT-ID	(Optional) Specifies the unit ID to display the rate limit configuration and statistics by sub-interface.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 : 1000 pps
Unit            Total     Drop
--------------  --------- ---------
1               50        0
3               50        0

Switch#
```

89-7 show cpu-protect type

This command is used to display the rate limit and statistics of CPU protection.

show cpu-protect type {*PROTOCOL-NAME* **[***UNIT-ID***] | unit** *UNIT-ID***}**

Parameters

PROTOCOL-NAME **[***UNIT-ID***]**	Specifies that the configured rate limit and statistics of the specified protocol on the CM-card and all existing IO-cards will be displayed if the optional unit ID is not specified. Otherwise, only the information on the specified unit ID will be displayed.
unit *UNIT-ID*	Specifies the unit ID to display the rate limit configuration and statistics.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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: 300  pps
Unit            Total     Drop
--------------  --------- ---------
1               30        0
3               30        0

Switch#
```

90. Secure File Transfer Protocol (SFTP) Server Commands

90-1 ip sftp server

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

ip sftp server

no ip sftp server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable the SFTP function globally. SFTP is a remotely secure file transfer protocol over a reliable data stream. Because SFTP itself does not provide authentication and security, the SFTP server runs as a sub-system of the SSH server. It is required to enable the SSH server by using the **ip ssh server** command to make SFTP work correctly. Disabling the SSH server or the SFTP server will cause all established SFTP sessions disconnected.

When the SFTP server is enabled on the switch, manage the files on the switch using various SFTP clients, like WinSCP, PSFTP, FileZilla, and more.

Example

This example shows how to enable the SFTP server.

```
Switch# configure terminal
Switch(config)# ip ssh server
Switch(config)# ip sftp server
Switch(config)#
```

90-2 ip sftp timeout

This command is used to configure the SFTP idle timer on the switch. To restore to the default value, use the **no** form of this command.

ip sftp timeout *SECONDS*

no ip sftp timeout

Parameters

SECONDS	Specifies the idle timer for the SFTP server. If the SFTP server detects no operation after the duration of idle timer for a specific SFTP session, the switch will close this SFTP session. The range is from 30 to 600 seconds.

Default

The default idle timer for SFTP sessions is 120 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to specify the idle timer for the SFTP server. The new setting will be applied to SFTP sessions established afterwards, the current connected SFTP sessions won't be affected. The cancel of an idle SFTP session takes no effect to the corresponding SSH Shell session. After all SSH sessions (SFTP session and Shell session) of a connection closed, the SSH connection will be closed.

Example

This example shows how to specify the idle timer for the SFTP server to 600 seconds.

```
Switch# configure terminal
Switch(config)# ip sftp timeout 600
Switch(config)#
```

90-3 show ip sftp

This command is used to display the SFTP server settings.

show ip sftp

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the SFTP server settings.

Example

This example shows how to display the global settings of the SFTP server.

```
Switch# show ip sftp
```

```
IP SFTP server      : Enabled
Protocol version    : 3
Idle time out       : 120 secs

Switch#
```

91. Secure Shell (SSH) Commands

91-1 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.
dsa	Specifies to generate the DSA key pair. The DSA key size is fixed as 1024 bit.
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.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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#
```

91-2 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command deletes 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#
```

91-3 ip ssh timeout

This command is used to configure the SSH control parameters on the switch. To restore the default values, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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)#
```

91-4 ip ssh server

This command is used to enable the SSH server function. Use the **no** 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable 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)#
```

91-5 ip ssh service-port

This command is used to specify the service port for SSH. Use the **no** command to return the service port to 23.

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.

Command Default Level

Level: 12.

Usage Guideline

This command configures the TCP port number 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)#
```

91-6 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the RSA or DSA public key pairs.

Example

This example shows how to information regarding 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 AADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s7l9H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Switch#
```

91-7 show ip ssh

This command is used to display the user SSH configuration settings.

show ip ssh

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to 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#
```

91-8 show ssh

This command is used to display the status of SSH server connections.

show ssh

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the SSH connections' status on the switch.

Example

This example shows how to display SSH connections' information.

```
Switch# show ssh

SID Ver. Cipher                       Userid           Client IP Address
--- --- --------------------------- ---------------- ------------------------
0   V2  3des-cbc/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.

91-9 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 restore the default authentication method.

ssh user *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

no ssh user *NAME* **authentication-method**

Parameters

user *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.

Command Default Level

Level: 12.

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 flash: c:/user1.pub
```

```
Switch(config)#
```

92. Secure Sockets Layer (SSL) Commands

92-1 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.

Command Default Level

Level: 12.

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.

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)#
```

92-2 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.
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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command allows administrators 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 doesn't 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 Ethernet0):!
[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 Ethernet0):!
[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 Ethernet0):!
[OK - 1289 bytes]
% PEM files import succeeded.

Switch(config)#
```

92-3 crypto pki trustpoint

This command is used to declare the trust-point that the switch will use. To delete all certificates and key pairs associated with the trust-point, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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 trustpimport TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

92-4 crypto pki certificate chain

This command is used to enter into 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter into certificate chain configuration mode. If the specified trust-point name doesn't exist, an error message will be displayed.

Example

This example shows how to enter into certificate chain configuration mode.

```
Switch# configure terminal
Switch(config)# crypto pki certificate chain TP1
Switch(trustpoint)#
```

92-5 primary

This command is used to assign a specified trust-point as the primary trust-point of the switch.

primary

no primary

Parameters

None.

Default

By default, this option is disabled.

Command Mode

CA-Trust-Point Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the primary command to specify a given trust-point as primary. This trust-point can be used as default trust-point when the application doesn't 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)#
```

92-6 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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#
```

92-7 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

When the name of the SSL service policy is not 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        : policy1
  Enabled CipherSuites :
    RSA_WITH_RC4_128_MD5,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 600
  Secure Trustpoint    : TP1

SSL Policy Name        : policy2
  Enabled CipherSuites :
    RSA_WITH_RC4_128_MD5,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_EXPORT_WITH_RC4_40_MD5
  Session Cache Timeout: 1200
  Secure Trustpoint    : TP2

Switch#
```

92-8 ssl-service-policy

This command is used to configure the SSL service policy.

ssl-service-policy *POLICY-NAME* **[ciphersuite [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-sha] [rsa-rc4-128-sha] [rsa-rc4-128-md5] [rsa-export-rc4-40-md5] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

no ssl-service-policy *POLICY-NAME* **[ciphersuite [dhe-dss-3des-ede-cbc-sha] [rsa-3des-ede-cbc-sha] [rsa-rc4-128-sha] [rsa-rc4-128-md5] [rsa-export-rc4-40-md5] | secure-trustpoint | session-cache-timeout]**

Parameters

POLICY-NAME	Specifies the name of the SSL service policy.
ciphersuite	(Optional) Specifies the cipher suites that should be used by the secure service when negotiating a connection with a remote peer. **dhe-dss-3des-ede-cbc-sha** - Use DH key exchange with 3DES-EDE-CBC encryption and SHA for message digest. **rsa-3des-ede-cbc-sha** - 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** - Use RSA key exchange with RC4 128-bit encryption for message encryption and SHA for message digest. **rsa-rc4-128-md5** - 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** - Use RSA EXPORT key exchange with RC4 40 bits for message encryption and MD5 for message digest. 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.
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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

93. sFlow Commands

93-1 sflow receiver

This command is used to configure a receiver for the sFlow agent. Receivers cannot be added to or removed from the sFlow agent. Use the **no** form of this command to reset one receiver to the default settings.

sflow receiver *INDEX* **[owner** *NAME***] [expiry {***SECONDS* **| infinite}] [max-datagram-size** *SIZE***] [host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}] [vrf** *VRF-NAME***] [udp-port** *PORT***]**

no sflow receiver *INDEX*

Parameters

INDEX	Specifies the index of the receivers.
owner *NAME*	(Optional) Specifies the owner name of the receiver with a maximum of 32 characters. The user cannot directly configure the owner as an empty string.
expiry *SECONDS*	(Optional) Specifies the expiration time for the entry. The parameter of the entry will reset when the timer expired. The range is from 0 to 2000000. The user cannot directly configure the expiry timer as 0.
infinite	(Optional) Specifies that the entry will not be expired.
max-datagram-size *SIZE*	(Optional) Specifies the maximum number of data bytes of a single sFlow datagram. The valid range is from 700 to 1400.
host *IP-ADDRESS*	(Optional) Specifies the IPv4 address of the remote sFlow collector.
host *IPV6-ADDRESS*	(Optional) Specifies the IPv6 address of the remote sFlow collector.
vrf *VRF-NAME*	(Optional) Specifies the name of the routing forwarding instance.
udp-port *PORT*	(Optional) Specifies the UDP port of the remote sFlow collector. The default is 6343. The range is from 1 to 65535.

Default

The default owner name is an empty string.

The expiry timer is 0 seconds.

The maximum datagram size is 1400 bytes.

The receiver IP address is 0.0.0.0.

The UDP port number is 6343.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The sFlow agent has a fix number of receivers distinguished by index. They are created in reset the state by the system and cannot be removed. Configure the owner of an entry before configuring other parameters of the entry. The owner of an entry can only be configured when the entry is in the reset state. The user cannot configure the owner name as an empty string. Once the owner is configured, it cannot be changed directly. It can only be reset by the **no sflow receiver** command.

Use the **no sflow receiver** command to reset the receiver. When a receiver expired, the receiver is disabled and the receiver entry will be reset to the default settings. The expiration timer starts to count down when its value is configured. The user cannot configure the expiry timer as 0.

Example

This example shows how to configure the receiver of index 1 with the owner name of collector1, a timeout value of 86400 seconds, size as 1400 bytes, remote sFlow collector's IP address as 10.1.1.2, and port number of 6343.

```
Switch# configure terminal
Switch(config)# sflow receiver 1 owner collector1 expiry 86400 max-datagram-size 1400
host 10.1.1.2 udp-port 6343
switch(config)#
```

93-2 sflow sampler

This command is used to create or configure a sampler for the sFlow agent. Use the **no** form of this command to delete one sampler.

sflow sampler *INSTANCE* **[receiver** *RECEIVER***] [inbound | outbound] [sampling-rate** *RATE***] [max-header-size** *SIZE***]**

no sflow sampler *INSTANCE*

Parameters

INSTANCE	Specifies the instance index if multiple samplers are associated with one interface. The valid range is from 1 to 65535.
receiver *RECEIVER*	(Optional) Specifies the receiver's index for this sampler. If not specified, the value is 0. The user cannot configure the value to 0.
inbound	(Optional) Specifies to sample ingress packets. This is the default direction of a sampler.
outbound	(Optional) Specifies to sample egress packets.
sampling-rate *RATE*	(Optional) Specifies the rate for packet sampling. The range is from 0 to 65536. 0 means disable. If not specified, the default value is 0.
max-header-size *SIZE*	(Optional) Specifies the maximum number of bytes that should be copied from sampled packets. The range is from 18 to 256. If not specified, the default value is 128.

Default

By default, no sampler is created.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command without keywords to create a default sampler or to reset an existing sampler to default values. Use the **no** form of this command with an instance to delete one sampler.

The user can only specify a receiver that has its owner name setup. If the receiver associated with the sampler has its owner name reset, the sampler will be reset to the default setting. The receiver ID of a default sampler is 0.

The user can configure an instance's mode to either inbound or outbound. If not specified, the default mode is inbound which will monitor the ingress packets.

An interface can be configured with multiple samplers. If multiple samplers are configured, the configured sampling rate can be different. But the sampling rate of all other samplers in the same direction must be multiples in power of 2 of the minimal configured sampling rate.

The sampling rate in operation may be automatically adjusted to a lower rate when the system is overloading.

Example

This example shows how to create the sampler of instance 1 with the receiver as 1, inbound, rate as 1024 and size as 128 bytes.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

93-3 sflow poller

This command is used to create or configure a poller for the sFlow agent. Use the **no** form of this command to delete a poller.

sflow poller *INSTANCE* **[receiver** *RECEIVER***] [interval** *SECONDS***]**

no sflow poller *INSTANCE*

Parameters

INSTANCE	Specifies the instance index if multiple pollers are associated with one interface. The range is from 1 to 65535.
receiver *RECEIVER*	(Optional) Specifies the receiver's index for this poller. If not specified, the value is 0. The user cannot configure the value to 0.
interval *SECONDS*	(Optional) Specifies the maximum number of seconds between successive polling samples. The range is from 0 to 120. 0 means disable. If not specified, the default is 0.

Default

By default, no poller is created.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command without keywords to create a default poller or to reset an existing poller to default values. Use the **n**o form of this command with an instance to delete one poller.

The user can only specify a receiver that has its owner name setup. If the receiver associated with the poller has its owner name is reset, the poller will be reset to the default setting.

Setting the polling interval to 0 disables the polling. An interface can be configured with multiple pollers.

Example

This example shows how to create the poller of instance 1 with receiver as 1 and interval as 20 seconds.

```
Switch# configure terminal
Switch(config)# interface ethernet 1/0/1
Switch(config-if)# sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

93-4 show sflow

This command is used to display sFlow information.

show sflow [agent | receiver | sampler | poller]

Parameters

agent	(Optional) Specifies to display sFlow agent information.
receiver	(Optional) Specifies to display information of all receivers.
sampler	(Optional) Specifies to display information of all samplers.
poller	(Optional) Specifies to display information of all pollers.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display sFlow information. If the MIB is not supported, the MIB version in the sFlow Agent Version string will be null. If the vendor changes, the organization name in the sFlow Agent Version string will change too.

Example

This example shows how to display all types of sFlow objects' information.

```
Switch# show sflow

sFlow Agent Version            : ;D-Link Inc.;1.00
sFlow Agent Address            : 10.1.1.1
sFlow Agent IPv6 Address       :


Receivers Information
Index                          : 1
Owner                          : collector1
```

```
Expire Time                    : 86500
Current Countdown Time         : 86122
Max Datagram Size              : 1400
Address                        : 10.1.1.2
VRF Name                       : vrf1
Port                           : 6343
Datagram Version               : 5

Index                          : 2
Owner                          : collector2
Expire Time                    : 86500
Current Countdown Time         : 86355
Max Datagram Size              : 1400
Address                        : 10.1.1.3
VRF Name                       :
Port                           : 6343
Datagram Version               : 5

Index                          : 3
Owner                          :
Expire Time                    : 0
Current Countdown Time         : 0
Max Datagram Size              : 1400
Address                        : 0.0.0.0
VRF Name                       :
Port                           : 6343
Datagram Version               : 5

Index                          : 4
Owner                          :
Expire Time                    : 0
Current Countdown Time         : 0
Max Datagram Size              : 1400
Address                        : 0.0.0.0
VRF Name                       :
Port                           : 6343
Datagram Version               : 5

Samplers Information
Interface Instance Receiver   Mode   Admin Rate  Active Rate  Max Header Size
--------- -------- -------- -------- ----------  -----------  ---------------
eth3/0/1    1         1     inbound     256        0              128
eth3/0/2    1         2     inbound     256        256            128
eth3/0/2    2         2     outbound    512        512            256

Pollers Information
Interface  Instance  Receiver  Interval
---------  --------  --------  --------
eth3/0/1     1          1        10
eth3/0/2     1          1        10
eth3/0/2     2          2        20

Switch#
```

This example shows how to display the sFlow agent's information. This sFlow agent does not support MIB and support IPv4 and IPv6.

```
Switch# show sflow agent

sFlow Agent Version            : ;D-Link Inc.;1.00
sFlow Agent Address            : 10.90.90.90
sFlow Agent IPv6 Address       : FE80::201:2FF:FE03:400

Switch#
```

Display Parameters

sFlow Agent Version	Indicates the MIB version, organization and software revision.
sFlow Agent Address	The IPv4 address of the sFlow agent.
sFlow Agent IPv6 Address	The IPv6 address of the sFlow agent.
Index	The index into Receivers.
Owner	The owner name.
Expire Time	The expiry time configured by user.
Current Countdown Time	The time (in seconds) remaining before stop of sampling and polling.
Max Datagram Size	The maximum number of data bytes of a single sFlow datagram.
Address	The IPv4/IPv6 address of the remote sFlow receiver.
VRF Name	The name of the routing forwarding instance.
Port	The UDP port of the remote sFlow receiver.
Datagram Version	The version of sFlow datagrams.
Interface	The interface on which the sampler is configured.
Instance	The Sampler instance index.
Receiver	The Receiver's INDEX for this Sampler.
Mode	The instance's mode which is inbound, or outbound, or inactive.
Admin Rate	The rate for packet sampling configured by user.
Active Rate	The active rate for packet sampling set to chip.
Max Header Size	The maximum number of bytes that should be copied from sampled packets.
Interface	The interface on which the poller is configured.
Instance	The Poller instance index
Receiver	The Receiver's INDEX for this Poller.
Interval	The maximum number of seconds between successive polling.

94. Simple Mail Transfer Protocol (SMTP) Commands

94-1 smtp server

This command is used to configure the SMTP server and port setting.

smtp server *IP-ADDRESS* **[vrf** *VRF-NAME***] [port** *PORT***]**

no smtp server [port]

Parameters

IP-ADDRESS	Specifies the IP address of the SMTP server.
PORT	Specifies the TCP port number used to contact the SMTP server. The default port number is 25. The valid range is from 1 and 65535.

Default

By default, this value is 25.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The system provides the service to send SYSLOG messages to email receivers via SMTP. Email messages will only be sent only when the mail server, recipient, and own mail address are configured. The switch acts as the SMTP client and sends the SYSLOG message to the SMTP server, then the server will delivers email messages to the recipient. Up to one SMTP server can be configured for a switch.

Example

This example shows how to configure the server IP to 172.18.208.9 and the TCP port to 587.

```
Switch# configure terminal
Switch(config)# smtp server 172.18.208.9 587
Switch(config)#
```

94-2 smtp self

This command is used to configure the email address which represent the switch that sends the email message. Use the **no** form of the command to remove the self email address.

smtp self *EMAIL-ADDRESS*

no smtp self

Parameters

self *EMAIL-ADDRESS*	Specifies the email address that which represents the switch.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the email address that represents the switch. Only one email address can be configured for this switch.

Example

This example shows how to configure the switch's email sender address as switch@domain.com.

```
Switch# configure terminal
Switch(config)# smtp self switch@domain.com
Switch(config)#
```

94-3 smtp recipient

This command is used to configure the recipient where the email will be sent. Use the **no** form of the command to remove a recipient.

smtp recipient *EMAIL-ADDRESS*

no smtp recipient {all | *EMAIL-ADDRESS***}**

Parameters

recipient *EMAIL-ADDRESS*	Specifies a recipient to receive the email.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The system provides the service to send SYSLOG messages to email receivers via SMTP. Use the **smtp recipient** command to configure the email address to receive the email message. By default, no messages will be sent. Use the **logging smtp** command to enable the sending of SYSLOG messages to the email recipients and configure the filtering criteria.

Example

This example shows how to add the receiver mail address as receiver@domain.com.

```
Switch# configure terminal
```

```
Switch(config)# smtp recipient receiver@domain.com
Switch(config)#
```

94-4 smtp interval

This command is used to configure the SMTP interval time. Use the **no** form of the command to recover to the default value.

smtp interval *MINUTES*

no smtp interval

Parameters

MINUTES	Specifies the SMTP sending interval. If set to 0, switch will send a mail for each event immediately.

Default

By default, this value is 30 minutes.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the SMTP sending interval that the switch uses.

Example

This example shows how to configure the interval to 10 minutes.

```
Switch# configure terminal
Switch(config)# smtp interval 10
Switch(config)#
```

94-5 show smtp

This command is used to display SMTP information.

show smtp

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display information of SMTP.

Example

This example shows how to display SMTP information.

```
Switch# show smtp

SMTP Server Address   : 172.18.208.9
SMTP Server Port      : 25
Self Mail Address     : switch@domain.com

Index  Mail Receiver Address
-----  ----------------------
1      receiver1@domain.com
2      receiver2@domain.com
3      receiver3@domain.com
4      receiver4@domain.com
5      receiver5@domain.com
6      receiver6@domain.com
7      receiver7@domain.com
8      receiver8@domain.com

Switch#
```

94-6 smtp send-testmsg

This command is used to check the reachability of the SMTP server.

smtp send-testmsg

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to check the reachability of the SMTP server. An email will be sent to all of the configured recipients.

Example

This example shows how to send a test mail to all users currently configured in the recipient list.

```
Switch# smtp send-testmsg

Subject: This is the test message subject!
Content: This is the test message content!

Sending mail, please wait!

Switch#
```

95. Simple Network Management Protocol (SNMP) Commands

95-1 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-ID	(Optional) Specifies the interface ID. If no interface is specified, then all interfaces will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display per interface link up/down trap state.

Example

This example shows how to display the interface's link up/down trap state for port eth1/0/1 to eth1/0/9.

```
Switch# show snmp trap link-status interface eth1/0/1-1/0/9

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#
```

95-2 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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#
```

95-3 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-ID	(Optional) Specifies the interface ID. If no interface is specified, then all ports will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the per port trap sending state.

Example

This example shows how to display the trap sending state for ports eth1/0/1 to eth1/0/9.

```
Switch# show snmp-server trap-sending interface eth1/0/1-1/0/9

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#
```

95-4 snmp-server

This command is used to enable the SNMP agent. Use the **no** 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.

Command Default Level

Level: 12.

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)#
```

95-5 snmp-server contact

This command is used to configure the system contact information for the device. Use the **no** command to remove the setting.

snmp-server contact *TEXT*

no snmp-server contact

Parameters

contact *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.

Command Default Level

Level: 12.

Usage Guideline

This command configures 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)#
```

95-6 snmp-server enable traps

This command is used to enable the sending of trap packets globally. Use the **no** command to disable the sending of trap packets.

snmp-server enable traps

no snmp-server enable traps

Parameters

None.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables the device to send the SNMP notification traps globally. To configure the router to send these SNMP notifications, enter the **snmp-server enable traps** command to enable the global setting.

Example

This example shows how to enable the SNMP traps global sending state.

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

95-7 snmp-server enable traps snmp

This command is used to enable the sending of all or specific SNMP notifications. To disable sending of all or specific SNMP notifications, use the **no** form of this command.

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 signifies 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.

Command Default Level

Level: 12.

Usage Guideline

This command controls 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 router 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)#
```

95-8 snmp-server location

This command is used to configure the system's location information Use the **no** command to remove the setting.

snmp-server location *TEXT*

no snmp-server location

Parameters

location *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.

Command Default Level

Level: 12.

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)#
```

95-9 snmp-server name

This command is used to configure the system's name information. Use the **no** command to remove the setting.

snmp-server name *NAME*

no snmp-server name

Parameters

NAME	Specifies the string that describes the host name information. The maximum length is 255 characters. As a suggestion do not configure the hostname longer than 10 characters.

Default

By default, this name is "Switch".

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)# system-name SiteA-switch
Switch(config)#
```

95-10 snmp-server trap-sending disable

This command is used to disable the port's trap sending state. Use the **no** command to disable the port's trap sending state.

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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to disable the port to send SNMP notification traps out of the configured port. If the sending is disabled, then 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 the notification traps out of Ethernet interface eth3/0/8.

```
Switch# configure terminal
Switch(config)# interface eth3/0/8
Switch(config-if)# snmp-server trap-sending disable
Switch(config-if)#
```

95-11 snmp-server service-port

This command is used to configure the SNMP UDP port number. Use the **no** form of this command to reset the UDP port number to default value.

snmp-server service-port *PORT-NUMBER*

no snmp-server service-port

Parameters

PORT-NUMBER	Specifies the UDP port number. The range is from 0 to 65535. Some numbers may conflict with other protocols.

Default

By default, this number is 161.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

95-12 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

95-13 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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 eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# no snmp trap link-status
Switch(config-if)#
```

95-14 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays 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

Codes: ro - read only, rw – Read Write

Community         access  view
----------------- ---- ------------------------------------------------------------
System             rw   sales-divison checked with IP access control list:
SalesDvision
public             ro   RD-division checked with IP access control list: HB5
Develop           ro   RD2
private           rw   Line2 checked with IP access control list: HQ

Total Entries: 4

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: 000000090200000000C025808

Switch#
```

95-15 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

When the username argument is not specified, all configured users will be displayed. The community string created will not displayed by this command.

Example

This example shows how SNMP users are displayed.

```
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#
```

95-16 snmp-server community

This command is used to configure the community string to access the SNMP. Use the **no** command to remove the community string,

snmp-server community [0 | 7] *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [***IP-ACL-NAME***]**

no snmp-server community [0 | 7] *COMMUNITY-STRING*

Parameters

0 *COMMUNITY-STRING*	(Optional) Specifies the community string in the plain text form with a maximum of 32 alphanumeric characters. This is the default option.
7 *COMMUNITY-STRING*	(Optional) Specifies the community string in the encrypted form.
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.
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.

Command Default Level

Level: 12.

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 the view is not specified, it is permitted to access all objects.

Example

This example shows how a MIB view “interfacesMibView” is created and a community string “comaccess” which can do read write access the interfacesMibView view is created.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.1.2 included
Switch(config)# snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

95-17 snmp-server engineID local

This command is used to specify the SNMP engine ID on the local device. Use the **no** command to revert the SNMP engine ID to the default.

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.

Command Default Level

Level: 12.

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 33220000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 3322
Switch(config)#
```

95-18 snmp-server group

This command is used to configure an SNMP group. Use the **no** 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
ReadGroup	SNMPv1	noauth	CommunityView	None	CommunityView
ReadGroup	SNMPv2c	noauth	CommunityView	None	CommunityView
WriteGroup	SNMPv1	noauth	CommunityView	CommunityView	CommunityView
WriteGroup	SNMPv2c	noauth	CommunityView	CommunityView	CommunityView

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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 mode, 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)#
```

95-19 snmp-server host

This command is used to specify the recipient of the SNMP notification. Use the **no** command to remove the recipient.

snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***] [version {1 | 2c | 3 {auth | noauth | priv}}]** *COMMUNITY-STRING* **[port** *PORT-NUMBER***]**

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

Parameters

IP-ADDRESS	Specifies the IPv4 address of the SNMP notification host.
IPV6-ADDRESS	Specifies the IPv6 address of the SNMP notification host.
VRF-NAME	Specifies the name of the routing forwarding instance.
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	Specifies to authenticate the packet but not to encrypt it.
noauth	Specifies not to authenticate and to encrypt the packet.
priv	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	Specifies the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 0 to 65535. Some port numbers may conflict with other protocols.

Default

By default, the version used is 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

95-20 snmp-server source-interface traps

This command is used to specify the interface whose IP address will be used as the source address for sending the SNMP trap packet. To revert to default setting, use the **no** form of this command.

snmp-server source-interface traps *INTERFACE-ID*

no snmp-server source-interface traps

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source address for sending the SNMP trap packet.

Default

The IP address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the interface whose IP address will be used as the source address for sending the SNMP trap packet.

Example

This example shows how to configure VLAN 100 as the sourcing interface for sending SNMP trap packets.

```
Switch# configure terminal
Switch(config)# snmp-server trap source-interface vlan100
Switch(config)#
```

95-21 snmp-server user

This command is used to create an SNMP user. Use the **no** command to remove an SNMP user.

snmp-server user *USER-NAME GROUP-NAME* **{v1 | v2c | v3 [encrypted] [auth {md5 | sha}** *AUTH-PASSWORD* **[priv** *PRIV-PASSWORD*]]} **[access** *IP-ACL-NAME*]

no snmp-server user *USER-NAME GROUP-NAME* **{v1 | v2c | v3}**

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.
v3	Specifies that the user uses the SNMPv3 security mode.
encrypted	(Optional) Specifies that the following password is in encrypted format.
auth	(Optional) Specifies the authentication level.
md5	Specifies to use HMAC-MD5-96 authentication.
sha	Specifies to use HMAC-SHA-96 authentication.
AUTH-PASSWORD	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 keyword **encrypted** is specified, the length is 32 for MD5 and 40 for SHA. The format is a hexadecimal value.
PRIV-PASSWORD	Specifies the private password in the plain-text form. This password is 8 to 16 octets. If the keyword **encrypted** 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.

Command Default Level

Level: 12.

Usage Guideline

To create a SMNP 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 the plain-text password is configured 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 the MD5 digest string is used instead of the plain text password.

```
Switch# configure terminal
Switch(config)# snmp-server user user1 public v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

95-22 snmp-server view

This command is used to create or modify a view entry. Use the **no** 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.

Command Default Level

Level: 12.

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)#
```

96. Single IP Management (SIM) Commands

96-1 sim

This command is used to enable single IP management. The **no** form of this command disables single IP management.

sim

no sim

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the single IP management function of the device and the **no** form of the command to disable the single IP management function of the device.

Example

This example shows how to enable single IP management.

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

96-2 sim role

This command is used to configure the device's single IP management role from Candidate to Commander or from Commander to Candidate.

sim role {commander [*GROUP-NAME***] | candidate}**

Parameters

commander	Specifies to configure the device to Commander switch.
GROUP-NAME	(Optional) Specifies to assign a name for the group when configuring the device to the Commander mode.
candidate	Specifies to configure the device to Candidate switch.

Default

By default, the single IP management group name is "default".

By default, the switch role is Candidate.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

There are 3 roles in the single IP management system: Candidate, Commander and Member.

The roles of Candidate and Commander can be specified by the user. The Member role can be specified by the command **sim group-member** on the commander switch.

The SIM group consists of the Commander switch and many member switches If the switch roles change, like Commander to Candidate, all of the members in the SIM group will be changed to Candidate.

Example

This example shows how to create a single IP management group.

```
Switch# configure terminal
Switch(config)# sim role commander my-group
Switch(config)#
```

96-3 sim group-member

This command is used to add one Candidate switch to the single IP management group. Use **no** form to remove one member from this single IP management group.

sim group-member *CANDIDATE-ID* **[***PASSWORD***]**

no sim group-member *MEMBER-ID*

Parameters

CANDIDATE-ID	Specifies one Candidate switch in one SIM group.
MEMBER-ID	Specifies one Member switch in one SIM group.
PASSWORD	Specifies the password of the Candidate switch.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

On the Commander switch, the Candidate switch can be joined to the group and it will be changed to the member switch. The Commander switch must pass the Candidate switch Level-15 password authentication.

Example

This example shows how to add one candidate switch to the single IP management group.

```
Switch# configure terminal
Switch(config)# sim group-member 1 secret
Switch(config)#
```

96-4 sim holdtime

This command is used to configure the hold-time duration in seconds. One switch (ether the Commander or Member switch) will clear the information of the other switch, after not receiving single IP management messages in the duration time. Use the **no** form to reset the hold-time to the default.

sim holdtime *SECONDS*

no sim holdtime

Parameters

SECONDS	Specifies the hold-time in seconds. The range is from 100 to255.

Default

By default, this value is 100 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

During the hold time, If no SIM protocol message were received, it will:

- For the Commander switch, clear Member switch information.
- For the Member switch, clear the Commander switch information and change the role to Candidate.

Example

This example shows how to configure the single IP management hold-time.

```
Switch# configure terminal
Switch(config)# sim holdtime 120
Switch(config)#
```

96-5 sim interval

This command is used to configure the SIM interval in seconds for single IP management protocol sending messages. Use the **no** form to set the interval as default.

sim interval *SECONDS*

no sim interval

Parameters

SECONDS	Specifies the interval value in seconds. The range is from 30 to 90.

Default

By default, this value is 30 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the SIM interval in seconds for single IP management protocol sending messages.

Example

This example shows how to configure the interval for the single IP management protocol.

```
Switch# configure terminal
Switch(config)# sim interval 60
Switch(config)#
```

96-6 sim management vlan

This command is used to configure SIM management VLAN. Use the **no** form of the command to revert to the default setting.

sim management vlan *VLAN-ID*

no sim management vlan

Parameters

VLAN-ID	Specifies the single IP management message VLAN.

Default

By default, this option is set the VLAN 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The single IP management group commander and member will send and receive the SIM message on the SIM management VLAN.

Example

This example shows how to configure the single IP management VLAN to 100.

```
Switch# configure terminal
```

```
Switch(config)# sim management vlan 100
Switch(config)#
```

96-7 sim remote-config

This command is used to remotely login and configure the single IP management group member or exit from the remote configuration.

sim remote-config {member *MEMBER-ID* **| exit}**

Parameters

MEMBER-ID	Specifies the member that login.
exit	Specifies to exit from the current configuring member.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The SIM Commander switch can login to its group members and configure them by the member ID. This command only can be used on the Commander switch.

Example

This example shows how to login the single IP management group member device.

```
Switch# sim remote-config member 1
Switch#
```

96-8 copy sim

This command is used to copy a file to single IP management group members.

copy sim *SOURCE-URL DESTINATION-URL* **[member** *MEMBER-LIST***]**

Parameters

SOURCE-URL	Specifies the source URL to be uploaded to the server. The source URL is located on the member switch. When the running configuration is specified as the source URL, the purpose is to upload the running configuration to the TFTP server. When the system log is specified as source URL, the system log can be retrieved to the TFTP server.
DESTINATION-URL	Specifies the destination URL for the file download. The destination URL is located on the member switch. When the running configuration

	is specified as the destination URL, the purpose is to download the running configuration from the TFTP server to member switches. When the firmware is specified as the destination URL, the purpose is to download the firmware from the TFTP server to member switches. The boot image on the member switches will be replaced by the downloaded file.
MEMBER-LIST	(Optional) Specifies the member switch to download the file. Multiple members can be specified at a time. Use ‘,’ to separate multiple IDs, or “-“ to denote a range of interface IDs.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used on Commander Switch to upload files to the server from member switches. In order to distinguish the different member switch’s ID, the file name will be appended to the member switch’s ID.

Example

This example shows how to download firmware to the member switch 1.

```
Switch# copy sim tftp://10.10.10.58/switch.had firmware member 1

Download firmware 10.10.10.58/ switch.had to member 1 ?(y/n)[n] y
Download Status:
ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

This example shows how to upload the system log from the member switch 1.

```
Switch# copy sim system-log tftp: //10.10.10.58/switchlog member 1

Upload system log  from member 1 to 10.10.10.58/switchlog ?(y/n)[n]y
Upload Status
ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

96-9 show sim

This command is used to display single IP management information.

show sim [{candidates [*CANDIDATE-ID*] | members [*MEMBER-ID*] | group [*COMMANDER-MAC*] | neighbor}]

Parameters

candidates	Specifies to display the information of Candidate switches.
CANDIDATE-ID	Specifies to display detailed information of a Candidate.
members	Specifies to display the information of Member switches.
MEMBER-ID	Specifies to display detailed information of a Member.
group	Specifies to display the information of other SIM Groups.
COMMANDER-MAC	Specifies to display detailed information of a Group.
neighbor	Specifies to display the neighbor information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display single IP management information.

Example

This example shows how to display detailed local SIM information on the Commander.

```
Switch# show sim

 Group Name          : my-group
 SIM Version         : VER-1.61
 Firmware Version    : 2.00.012
 Management VLAN     : 100
 Device  Name        :
 MAC Address         : 00-02-01-03-01-03
 Platform            : DXS-3600
 SIM State           : Enabled
 Role State          : Commander
 Discovery Interval  : 60 sec
 Hold Time           : 120 sec

Switch#
```

This example shows how to display detailed local SIM information on the Member switch.

```
Switch# show sim

 SIM Version         : VER-1.61
 Firmware Version    : 2.00.012
 Device Name         :
 MAC Address         : EE-FF-00-00-12-12
```

```
 Platform           : DXS-3600
 SIM State          : Enabled
 Role State         : Member
 Discovery Interval : 30 sec
 Hold Time          : 100 sec
----------------CS Info----------------
 CS Group Name   : my-group
 CS MAC Address  : 00-02-01-03-01-03
 CS Hold Time    : 90 s

Switch#
```

This example shows how to display the SIM member list.

```
Switch# show sim members
Member                                          Hold  Firmware
ID    MAC Address         Platform       Time  Version   Device Name
-------------------------------------------------------------------
   1    00-01-00-00-12-12 DXS-3600         100   2.00.012
   2    00-02-00-00-12-13 DXS-3600         80    2.00.012

Total Entries : 2

Switch#
```

This example shows how to display one of the SIM member's information in detail.

```
Switch# show sim members 1

Sim Member Information :
Member ID             : 1
Firmware Version      : 2.00.012
Device Name           :
MAC Address           : 00-01-00-00-12-12
Platform              : DXS-3600
Hold Time             : 100 sec

Switch#
```

This example shows how to display the SIM candidate list.

```
Switch# show sim candidates

Candidate                                       Hold  Firmware
ID      MAC Address         Platform     Time  Version     Device Name
-------------------------------------------------------------------
     1      EE-FF-00-00-12-12 DXS-3600       90    2.00.012

Total Entries : 1

Switch#
```

This example shows how to display one of the SIM candidate's information in detail.

```
Switch# show sim candidates 1

 Sim Candidate Information :
 Candidate ID          : 1
 Firmware Version      : 2.00.012
 Device Name           :
 MAC Address           : EE-FF-00-00-12-12
 Platform              : DXS-3600
 Hold Time             : 100 sec

Switch#
```

This example shows how to display group information in a summary.

```
Switch# show sim group
* -means Commander switch.

SIM Group Name : default
                                          Hold   Firmware
ID  MAC Address         Platform        Time  Version    Device Name
-------------------------------------------------------------------
*1  00-02-00-00-08-12 DXS-3600         40     2.00.012
 2  00-07-15-34-00-50
 3  00-01-02-03-00-10

SIM Group Name : SIM2
                                          Hold   Firmware
ID  MAC Address         Platform        Time  Version    Device Name
-------------------------------------------------------------------
*1  00-01-02-03-04-11 DXS-3600         40    2.00.012
 2  00-55-55-00-55-11

Total Entries : 2

Switch#
```

This example shows how to display SIM group detailed information.

```
Switch# show sim group 00-02-00-00-08-12

Sim Group Information :

[*** Commander Info ***]

Group Name : default
MAC Address           : 00-02-00-00-08-12
Device Name           :
Firmware Version      : 2.00.012
Platform              : DXS-3600
Number of Members     : 2
Hold Time             : 100 sec

[*** Member Info (1/2)***]
MAC Address    : 00-07-15-34-00-50
```

```
[*** Member Info (2/2)***]
MAC Address    : 00-01-02-03-00-10

Switch#
```

This example shows how to display SIM neighbors' summary.

```
Switch# show sim neighbor

Port   MAC Address        Role
-----------------------------------
1    00-02-00-00-08-12  Member
2    00-01-00-00-12-12  Member
2    EE-FF-00-00-12-12  Candidate

Total Entries : 3

Switch#
```

97. Spanning Tree Protocol (STP) Commands

97-1 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Using this command the port protocol migrating state machine will be forced 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#
```

97-2 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*	Specifies the interface ID to display.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the

	comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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

Protocol state: Enabled
protocol mode: RSTP
NNI BPDU Address: Dot1d(01-80-C2-00-00-00)
Root ID Priority      : 4096
    Address        : 00-04-9B-78-08-00
 Hello Time      : 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
Bridge ID Priority    : 4096 (priority 4096 sys-id-ext 0)
       Address        : 00-04-9B-78-08-00
       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#
```

97-3 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 *INTERFACE-ID*	Specifies the interface ID to display.

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

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 for interface eth3/0/1.

```
Switch# show spanning-tree configuration eth3/0/1

eth3/0/1
Spanning tree state: enabled
Port path cost: 4,
Port priority: 128,
   Link type: auto
   Port fast: edge
   Hello time: 2 seconds
   Guard root: disabled
   TCN filter: enabled
Bpdu forward: enabled

Switch#
```

97-4 snmp-server enable traps stp

This command is used to enable the spanning tree to send SNMP notifications for STP. Use the **no** form of the 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the sending of notification traps. When using this command with no parameters specified, both STP notification types are enabled or disabled.

Example

This example shows how to enable the router to send all STP 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 stp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

97-5 spanning-tree global state

This command is used to enable or disable the STP's global state. Use the **no** form to disable the STP's global 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.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the global configuration mode to enable the global spanning-tree function.

Example

This example shows how to enable the spanning-tree function.

```
Switch# configure terminal
Switch(config)# spanning-tree global state enable
Switch(config)#
```

97-6 spanning-tree (timers)

This command is used to configure the Spanning Tree timer value. Use the **no** form of the command to restore the default setting.

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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

97-7 spanning-tree state

This command is used to enable or disable the STP operation. Use the **no** command to revert to 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.

Command Default Level

Level: 12.

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 Ethernet interface eth3/0/1.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# spanning-tree state enable
Switch(config-if)#
```

97-8 spanning-tree cost

This command is used to configure the value of the port path-cost on the specified port. Use the **no** 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.

Command Default Level

Level: 12.

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 for Ethernet interface eth1/0/7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree cost 20000
Switch(config-if)#
```

97-9 spanning-tree guard root

This command is used to enable the root guard mode. To return to the default settings, use the **no** form of this command.

spanning-tree guard root

no spanning-tree guard root

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 Ethernet interface eth3/0/1 from being a root port.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# spanning-tree guard root
Switch(config-if)#
```

97-10 spanning-tree link-type

This command is used to configure a link-type for a port. To return to the default settings, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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 for port eth1/0/7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree link-type point-to-point
Switch(config-if)#
```

97-11 spanning-tree mode

This command is used to configure the STP mode. To return to the default settings, use the **no** form of this command.

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.

Command Default Level

Level: 12.

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)#
```

97-12 spanning-tree portfast

This command is used to specify the port's fast mode. Use the **no** form of the 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 **network**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 eth1/0/7 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)#
```

97-13 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 **no** form of this command to reset to the default priority.

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.

Command Default Level

Level: 12.

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 for port eth1/0/7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree port-priority 0
Switch(config-if)#
```

97-14 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.

Command Default Level

Level: 12.

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 command **spanning-tree mst priority** 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)#
```

97-15 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.

Command Default Level

Level: 12.

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 eth1/0/7.

```
Switch# configure terminal
Switch(config)# interface eth1/0/7
Switch(config-if)# spanning-tree tcnfilter
Switch(config-if)#
```

97-16 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 the command to restore 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.

Command Default Level

Level: 12.

Usage Guideline

This command specifies 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)#
```

97-17 spanning-tree forward-bpdu

This command is used to enable the forwarding of the spanning tree BPDU. Use the **no** form of the 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.

Command Default Level

Level: 12.

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 eth6/0/1
Switch(config-if)# spanning-tree forward-bpdu
Switch(config-if)#
```

97-18 spanning-tree nni-bpdu-address

This command is used to configure the destination address of the STP BPDU in the service provider site. Use the **no** form of the command to revert to the default setting

spanning-tree nni-bpdu-address {dot1d | dot1ad}

no spanning-tree nni-bpdu-address

Parameters

dot1d	Specifies to use the Customer Bridge Group Address (01-80-C2-00-00-00) as the destination address of the STP BPDU.

dot1ad	Specifies to use Provider Bridge Group Address (01-80-C2-00-00-08) as the destination address of the STP BPDU.

Default

By default, the Customer Bridge Group Address is used as the destination address of the STP BPDU.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Generally, the Customer Bridge Group Address is used as the destination address of the STP BPDU. This command is used to designate the destination address of the STP BPDU in the service provider site. It will only take effect on the VLAN trunk ports, which behave as the NNI ports in the service provider site.

This configuration will take effect for all the spanning-tree modes.

Example

This example shows how to configure using the **dot1ad** address as the destination address of the BPDU on the VLAN trunk port.

```
Switch# configure terminal
Switch(config)# spanning-tree nni-bpdu-address dot1ad
Switch(config)#
```

98. Stacking Commands

98-1 stack

This command is used to enable the daisy-chain stacking function and use the **no stack** command to disable the daisy-chain stacking function.

stack

no stack

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The ports on a stackable switch unit, used to chain with other switch units, can either work as stacking ports or work as ordinary Ethernet ports based on the setting of the stack command. The stack command setting of a switch unit must be enabled before the switch unit can be chained with other switch units. The setting will be saved in the individual switch unit if the user saves the configuration.

Example

This example shows how to enable stacking mode.

```
Switch# stack

WARNING: The command does not take effect until the next reboot.

Switch#
```

98-2 stack renumber

This command is used to manually assign a unit ID to a switch unit. Use the **no** form of the command to set the unit ID of the switch to auto-assigned.

stack *CURRENT-UNIT-ID* **renumber** *NEW-UNIT-ID*

no stack *CURRENT-UNIT-ID* **renumber**

Parameters

CURRENT-UNIT-ID	Specifies the switch unit being configured.
NEW-UNIT-ID	Specifies the new unit ID assigned to the switch.

Default

The unit ID is assigned automatically.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Initially, a switch unit has no unit ID assigned. When this switch unit is initialized or is added to a stack, it will get a unit ID auto-assigned by the master unit. After a unit ID was assigned, the unit ID can be kept in configuration file by issuing the **copy running-config startup-config** command and will be used after the next reboot.

The user can use this command to re-assign a unit ID to the specified switch unit. The assigned unit ID will be used after the next reboot. The switch unit cannot be added to a switch stack if its unit ID is conflicting with an existing switch unit in the stack.

The master unit automatically assigns unit IDs to switch units based on the following rules:

- If the unit ID of the master unit is auto-assigned, it will get 1 as its unit ID.
- If a switch unit to be added to the stack has a unit ID conflicting with a unit ID of a switch unit already added, then this switch unit ID cannot be successfully added.

Example

This example shows how to configure the renumbered unit ID of a switch unit 2 to 3.

```
Switch# stack 2 renumber 3

WARNING: The command does not take effect until the next reboot.

Switch#
```

98-3 stack priority

This command is used to configure the priority of the switch stacking unit. Use the **no** form of the command to set the priority to default.

stack *CURRENT-UNIT-ID* **priority** *NEW-PRIORITY-NUMBER*

no stack *CURRENT-UNIT-ID* **priority**

Parameters

CURRENT-UNIT-ID	Specifies the switch stacking unit being configured.
NEW-PRIORITY-NUMBER	Specifies the priority assigned to the switch stacking unit. The lower number means a higher priority. The range is between 1 and 63.

Default

By default, this value is 32.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the priority for the specified switch unit. When switch units are daisy-chained together as a stack, the unit with the best priority will be elected as the master. The unit with the next best priority will be elected as the backup master. A lower value means the higher priority. When two switch units have the same priority, the unit with the smaller MAC address will get the higher priority. The new priority setting will be saved in individual switch units when the user saves the configuration.

Example

This example shows how to configure the priority of the switch unit 2 to 10.

```
Switch# stack 2 priority 10
Switch#
```

98-4 stack preempt

This command is used to enable preemption of the master role to come into play when a unit with a better priority is added to the switch later. Use the **no** form of the command to disable preemption.

stack preempt

no stack preempt

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

When this command is disabled, the unit that assumes the master role will not change when units with a better priority are added to the stack. If this command is enabled, then the unit that assumes the master role will change as units with a better priority are added to the stack.

Example

This example shows how to enable preemption.

```
Switch# stack preepmt
Switch#
```

98-5 show stack

This command is used to display the stacking information.

show stack

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the stacking information.

Example

This example shows how to display stacking information.

```
Switch#show stack

Stacking mode  : Enabled
Stack Preempt: Enable

Topology     :Duplex_Chain
My Box ID    :3
Master ID    :3
BK Master ID :1
Box Count    :2

 Box User  Module             Prio-                        Prom        Runtime    H/W
 ID  Set    name        Exist rity        MAC            Version     Version
Version
 --- ----  ---------- ----- ---- ------------------ ---------- --------- --------
 1    Auto BOX-TYPE    Exist 32    00-22-55-44-77-11  1.10.008   2.00.012 B1
 2     -    NOT_EXIST    No
 3    User BOX-TYPE    Exist  0    00-00-11-33-66-33  1.10.008   2.00.012 B1
 4    -     NOT_EXIST    No

Switch#
```

99. Storm Control Commands

99-1 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 restore the function to its 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 that when the action is configured as the **shutdown** mode, the unicast refers to both known and unknown unicast packet, 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 1 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 1 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 1 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.

Command Default Level

Level: 12.

Usage Guideline

Use the storm control function to protect the network from a 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.

Example

This example shows how to enable broadcast storm control on eth3/0/1 and eth3/0/2. It sets the threshold of eth3/0/1 to 500 packets per second with the shutdown action and sets the threshold of the interface port 3.2 to 70% with the drop action.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# storm-control broadcast level pps 500
Switch(config-if)# storm-control action shutdown
Switch(config)# interface eth3/0/2
Switch(config-if)# storm-control broadcast level 70 60
Switch(config-if)# storm-control action drop
Switch(config-if)#
```

99-2 storm-control polling

This command is used to configure the polling interval of received packet counts. Use the **no** form of this command to restore to its 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 1 and 300 seconds.
retries *NUMBER*	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.

Command Default Level

Level: 12.

Usage Guideline

Use this 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)#
```

99-3 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 port's interface ID.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
broadcast	Specifies to display the current broadcast storm setting.
multicast	Specifies to display the current multicast storm setting.
unicast	Specifies to display the current unicast (DLF) storm setting.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the interface ID is not specified, all interfaces configurations will be displayed.

If the packet type is not specified, all types of storm control settings will be displayed.

Example

This example shows how to display the current broadcast storm control settings.

```
Switch# show storm-control interface range ethernet 3/0/1-3/0/6 broadcast

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Interface    Action    Threshold         Current    State
-------------------------------------------------------------
eth3/0/1     Drop      500/300 pps       200 pps    Forwarding
eth3/0/2     Drop      80/64 %           20 %       Forwarding
eth3/0/3     Drop      80/64 %           70 %       Dropped
eth3/0/4     Shutdown  60/50 %           20 %       Forwarding
eth3/0/5     None      60000/50000 kbps  2000 kbps  Forwarding
eth3/0/6     None      -                 -          Inactive
```

```
Total Entries: 6

Switch#
```

This example shows how to display all interface settings for the range from port 3/0/1 to port 3/0/2.

```
Switch# show storm-control interface eth3/0/1-2

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Trap                      : Disabled
Interface      Storm         Action      Threshold     Current    State
---------------------- ----------------------------------------------
eth3/0/1      Broadcast     Drop         80/64 %       50%        Forwarding
eth3/0/1      Multicast     Drop         80/64 %       50%        Forwarding
eth3/0/1      Unicast       Drop         80/64 %       50%        Forwarding
eth3/0/2      Broadcast     Shutdown     500/300 pps   -          Error Disabled
eth3/0/2      Multicast     Shutdown     500/300 pps   -          Error Disabled
eth3/0/2      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.

100. Super VLAN Commands

100-1 supervlan

This command is used to configure the VLAN as a super VLAN. Use **no** command to remove the super VLAN assignment.

supervlan

no supervlan

Parameters

None.

Default

None.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to specify a VLAN as a super VLAN. Super VLANs are used to aggregate multi sub-VLANs (Layer 2 broadcast domains) into IP subnets. A super VLAN cannot have any physical member port. A super VLAN cannot be a sub-VLAN at the same time. Once an IP interface is bound to a super VLAN, the proxy ARP will be enabled automatically on the interface for communication between its sub-VLANs. Multiple super VLANs can be configured and each super VLAN can consist of multiple sub-VLANs.

Private VLANs and super VLANs are mutually exclusive. A private VLAN cannot be configured as a super VLAN.

Layer 3 routing protocols, VRRP, multicast protocols, and the IPv6 protocol cannot run on a super VLAN interface.

Example

This example shows how to configure VLAN 10 as a super VLAN.

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# supervlan
   WARNING: Proxy ARP will be enabled automatically on this super VLAN.
Switch(config-vlan)#
```

100-2 subvlan

This command is used to add sub-VLANs to a super VLAN. Use the **no** command to remove sub-VLANs.

subvlan *VLAN-ID* **[, | -]**

no subvlan [*VLAN-ID* **[, | -]]**

Parameters

VLAN-ID	Specifies the ID of the VLAN as a sub-VLAN. The valid VLAN ID 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 required before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is required before and after the hyphen.

Default

None.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A sub-VLAN is a Layer 2 broadcast domain. This command is used to configure the sub-VLANs of a super VLAN. A sub-VLAN can only belong to one super VLAN. Private VLANs and Super VLANs are mutually exclusive.

Example

This example shows how to configure VLANs 5, 6 and 7 as the sub-VLANs of the super VLAN 10.

```
Switch# configure terminal
Switch(config)# vlan 10
Switch(config-vlan)# supervlan
Switch(config-vlan)# subvlan 5-7
Switch(config-vlan)#
```

100-3 subvlan-address-range

This command is used to configure the IP address range of a sub-VLAN. Use the **no** command to remove the IP address range of a sub-VLAN.

subvlan-address-range *START-IP-ADDRESS END-IP-ADDRESS*

no subvlan-address-range [*START-IP-ADDRESS END-IP-ADDRESS***]**

Parameters

START-IP-ADDRESS	Specifies the start IP address of this sub-VLAN.
END-IP-ADDRESS	Specifies the end IP address of this sub-VLAN.

Default

None.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only applicable on a sub-VLAN and is used to configure the IP address range of a sub-VLAN. Configuring IP address range(s) of a sub-VLAN can reduce the overhead when the switch is the ARP proxy between sub-VLANs. The wrong configuration of IP address ranges may cause IP traffic not to be routed correctly. A sub-VLAN can have one or more IP address ranges. The configured IP address range should not overlap with the existed address ranges of other sub-VLANs and must belong to the subnet of the super VLAN interface. Within a sub-VLAN, the configured IP address range will be merged into other range(s) if applicable.

Example

This example shows how to configure the IP address range of the sub-VLAN 5.

```
Switch# configure terminal
Switch(config)# vlan 5
Switch(config-vlan)# subvlan-address-range 192.168.10.1 192.168.10.50
Switch(config-vlan)#
```

100-4 show supervlan

This command is used to display the configuration of the super VLAN and its sub-VLANs.

show supervlan [*VLAN-ID* **[, | -]]**

Parameters

VLAN-ID	(Optional) Specifies the ID of the super VLAN to display.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is required before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is required before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the configuration of the super VLAN and its sub-VLANs.

Example

This example shows how to display the configuration of all super VLANs.

```
Switch# show supervlan
```

```
SuperVLAN ID SubVLAN ID SubVLAN Status  SubVLAN IP Address Range
------------ --------- --------------  --------------------------------
10           5          Active          192.168.10.1  - 192.168.10.50
             6          Inactive        192.168.10.51 - 192.168.10.60
             7          Inactive        192.168.10.61 - 192.168.10.70

Switch#
```

101. Switch Controller Commands

101-1 packet-forwarding asf

This command is used to enable the Alternative Store and Forward (ASF) feature. It allows packets to be sent in a cut-through manner. Use the **no** command to disable the ASF feature. When ASF is disabled, all packets are sent in the store and forward mode.

packet-forwarding asf

no packet-forwarding asf

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

ASF is used to reduce the latency for large packets. When ASF is enabled, packets can be forwarded before it has been entirely received. To avoid under runs, ASF takes place only when all the below conditions are met:

- The ingress port speed is faster or equal to that of the egress port.
- The packet size is larger than the pre-defined value.

Example

This example shows how to enable the ASF feature.

```
Switch# configure terminal
Switch(config)# packet-forwarding asf
Switch(config)#
```

102. Switch Port Commands

102-1 duplex

This command is used to configure the physical port interface's duplex setting. Use the **no** form of command to revert to the default setting.

duplex {full | half | auto} [rj45 | sfp]

no duplex [rj45 | sfp]

Parameters

full	Specifies that the port operates in the full-duplex mode.
half	Specifies that the port operates in the half-duplex mode.
auto	Specifies that the port's duplex mode will be determined by auto-negotiation.
rj45	(Optional) Specifies to configure the duplex for RJ45 media. For combo ports, if RJ45 or SFP is not specified, RJ45 is implied.
sfp	(Optional) Specifies to configure the duplex for SFP media.

Default

The duplex mode will be set as automatic for 1000BASE-T interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

For 1000BASE-T modules, if the speed is set to 1000, then the duplex mode cannot be set to half-duplex. If the duplex mode is set to half-duplex, then the speed cannot be set to 1000.

Auto-negotiation will be enabled if either the speed parameter is set to auto or the duplex parameter is set to auto if the speed parameter is set to auto and the duplex parameter is set to the fixed mode only the speed will be negotiated. The advertised capability will be configured to the duplex mode combined with all the possible speeds. If the speed is to set to a fixed speed and duplex is set to auto, only the duplex mode is negotiated. The advertised capability will be both full and half-duplex mode combined with the configured speeds.

Example

This example shows how to configure the interface eth1/1/1 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 eth1/1/1
Switch(config-if)# speed 100
Switch(config-if)# duplex auto
Switch(config-if)#
```

102-2 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.

Command Default Level

Level: 12.

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.

If no option is selected for the direction, both send and receive is used.

Example

This example shows how to enable the flow control on interface eth1/0/1.

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

102-3 media-type

This command is used to configure the media of a combo port that is selected for connection. Use the **no** form of command to revert to the default setting.

media-type {auto-select | rj45 | sfp}

no media-type

Parameters

auto-select	Specifies that the media type is selected based on the connection.
rj45	Specifies that the RJ45 media type is selected for the connection. SFP/SFP+ connection is disabled.
sfp	Specifies that the SFP/SFP+ media type is selected for the connection. RJ45 connection is disabled.

Default

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

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can only be applied to combo ports.

Example

This example shows how to configure the media type for interface eth1/1/1 to RJ45.

```
Switch# configure terminal
Switch(config)# interface eth1/1/1
Switch(config-if)# media-type rj45
Switch(config-if)#
```

102-4 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.

Command Default Level

Level: 12.

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 of interface eth1/1/1 to auto:

```
Switch# configure terminal
Switch(config)# interface eth1/1/1
Switch(config-if)# mdix auto
Switch(config-if)#
```

102-5 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.

NOTE: 10G does not support speed configurations of 10Mbps and 100Mbps.

speed {10 | 100 | 1000 [master | slave] | 10giga [master | slave] | 40giga | auto [*SPEED-LIST*]} [rj45 | sfp]

no speed [rj45 | sfp]

Parameters

10	Specifies to force the speed to 10Mbps.
100	Specifies to force the speed to 100Mbps.
1000	Specifies that for copper ports, it forces the speed to 1000Mbps and the user must manually set that the port operates as master or slave. Specifies that for fiber ports (1000BASE-SX/LX), the port will disable the auto-negotiation.
master | slave	Specifies the port operates as master or slave timing. This parameter is only applicable to 1000BASE-T connections.
10giga	Specifies to force the speed to 10Gbps.
master | slave	Specifies the port operates as master or slave timing. This parameter is only applicable to 10GBASE-T connections.
40giga	Specifies to force the speed to 40Gbps.
auto	Specifies that for copper ports, it specifies to determine the speed and flow control via auto-negotiation with its link partner. Specifies that for fiber ports (1000BASE-SX/LX), it enables the auto-negotiation option. Auto-negotiation will start to negotiate the clock and flow control with its link partner.
SPEED-LIST	(Optional) Specifies a list of speeds that the switch will only auto-negotiate to. The speed can be **1000**, and/or **10giga**. Use a comma (,) to separate multiple speeds. If the speed list is not specified, all speed will be advertised.
rj45	(Optional) Specifies to configure speed for RJ45 media. For combo

	ports, if RJ45 or SFP/SFP+ is not specified, RJ45 is used.
sfp	(Optional) Specifies to configure speed for SFP/SFP+ media.

Default

By default, the speed will be automatic for 1000BASE-T and 10GBASE-T interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the specified speed is not supported by the hardware, error messages will be returned. For a 1000BASE-T connection, if the speed is specified to 1000Mbps, the port must be configured as master or slave. For a 10GBASE-T connection, if the speed is specified to 10Gbps, the port must be configured as master or slave.

If speed is set to 1000Mbps, 10Gbps, or 40Gbps then the duplex mode cannot be set to half-duplex. If the duplex mode is set to half-duplex, then the speed cannot be set to 1000Mbps, 10Gbps or 40Gbps.

Auto-negotiation will be enabled if either the speed parameter is set to **auto**, or the duplex parameter is set to **auto**. If the speed parameter is set to auto, and the duplex parameter is set to the fixed mode. Only the speed will be negotiated. The advertised capability will be configured to the duplex mode combined with all the possible speeds. If the speed is to set to a fixed speed and duplex is set to auto, only the duplex mode is negotiated. The advertised capability will be both full and half-duplex mode combined with the configured speeds.

For 10GBASE-R connections, if auto-negotiation is enabled, the system will automatically configure the speed (1000M or 10G) according to the type of SFP/SFP+.

Example

This example shows how to configure eth1/1/1 to only auto-negotiate to 10Mbps or 100Mbps.

```
Switch# configure terminal
Switch(config)# interface eth1/1/1
Switch(config-if)# speed auto 10,100
Switch(config-if)#
```

103. System File Management Commands

103-1 boot config

This command is used to specify the file that will be used as the configuration file for the next boot.

boot config *URL*

Parameters

URL	Specifies the URL of the file to be used as the startup configuration file.

Default

By default, the *config.cfg* file is used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

The command is used to specify the startup configuration file. The default startup configuration file is *config.cfg*. 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 ‘switch-config.cfg’ as the startup configuration file.

```
Switch# configure terminal
Switch(config)# boot config c:/switch-config.cfg
Switch(config)#
```

103-2 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] *URL*

Parameters

check	(Optional) Specifies to display the firmware information for the specified file. This information includes the version number and model description.
URL	Specifies the URL of the file to be used as the boot image file.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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.

The backup image is decided automatically and is the newest valid image other than the boot-up one.

Example

This example shows how to specify that the switch should use the image file named ‘switch-image1.had’ as the boot image file for the next startup.

```
Switch# configure terminal
Switch(config)# boot image c:/switch-image1.had
Switch(config)#
```

This example shows how to check a specified image file called “c:/runtime.switch.had”. The checksum of the image file has been verified is okay and the information of the image file is displayed.

```
Switch# configure terminal
Switch(config)# boot image check c:/runtime.switch.had

----------------------
Image information
----------------------
Version    : 2.00.012
Description: D-Link Gigabit Ethernet Switch

Switch(config)#
```

This example shows how to checks a specified image file called “runtime.wrongswitch.had”. The checksum of the image file has been verified wrong and an error message is displayed.

```
Switch# configure terminal
Switch(config)# boot image check runtime.wrongswitch.had
ERROR: Invalid firmware image.
Switch(config)#
```

103-3 clear running-config

This command is used to clear the system’s running configuration.

clear running-config

Parameters

None.

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 15.

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, but not the stacking information. 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 all of system configuration as factory default setting
including IP parameters.
Clear running configuration? (y/n) [n] y

Switch#
```

103-4 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

Privilege EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to clear the system's configuration, including stacking information. 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 all of system configuration as factory default setting
including IP parameters and stacking information.
Clear running configuration, save, reboot? (y/n) [n] y
Saving configurations and logs to NV-RAM......   Done
Please wait, the switch is rebooting...
```

103-5 configure replace

This command is used to replace the current running configuration with the indicated configuration file.

configure replace {{tftp: //location/filename | rcp: //username@location/filename | ftp: //username:password@location:tcpport/filename} [vrf *VRFNAME***] | flash:** *FILENAME***} [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.
rcp:	Specifies that the configuration file is from the RCP server.
//username@location/filename	Specifies the URL of the configuration file on the RCP server.
ftp:	Specifies that the configuration file is from the FTP server.
//username:password@ location:tcpport/filename	Specifies the URL of the configuration file on the FTP server.
vrf *VRFNAME*	(Optional) Specifies the VRF name.
flash:	Specifies that the configuration file is from the NVRAM of the device.
FILENAME	Specifies the name of the configuration file stored in the NVRAM.
force	(Optional) Specifies to execute the command immediately with no confirmation needed.

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used 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 download the “config.cfg” from the RCP server and replace the current running configuration with it.

```
Switch#configure replace rcp: //User@10.0.0.66/config.cfg vrf dlink

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 rcp://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 download the “config.cfg” from the FTP server and replace the current running configuration with it. Execute the command immediately without confirmation.

```
Switch# configure replace ftp: //User:123@10.0.0.66:80/config.cfg force

 Accessing ftp: //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 specified configuration file “config.cfg” stored in the NVRAM of the device. Execute the command immediately without confirmation.

```
Switch# configure replace flash: config.cfg force

 Executing script file config.cfg ......
 Executing done

Switch#
```

103-6 copy

This command is used to copy a file to another file.

copy *SOURCE-URL DESTINATION-URL*

copy *SOURCE-URL* **{tftp: [***//LOCATION/DESTINATION-URL***] | ftp: [***//USER-NAME***:***PASSWORD@LOCATION***:***TCP-PORT/DESTINATION-URL***] | rcp: [***//USER-NAME@LOCATION/DESTINATION-URL***]} [vrf** *VRF-NAME***]**

copy {tftp: [*//LOCATION/SOURCE-URL***] | ftp: [***//USER-NAME***:***PASSWORD@LOCATION***:***TCP-PORT/SOURCE-URL***] | rcp: [***//USER-NAME@LOCATION/SOURCE-URL***]} [vrf** *VRF-NAME***]** *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 or saved as the file in the file system. If **attack-log** *UNIT-ID* is specified as the *SOURCE-URL*, the purpose is to upload one unit’s 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: [***PATH-FILE-NAME***]** is specified as the *DESTINATION-URL*,

	the purpose is to specify the copied file in the file system. If the input relative path is specified, the file will be downloaded to all units in stack and stored in the current path of each unit. If the input absolute path is specified, the file will be downloaded to the place which of the absolute path indicates. If there is no unit information in the absolute path, the master unit will be assigned.
LOCATION	Specifies the IPv4 address or IPv6 address of the TFTP/FTP/RCP server.
USER-NAME	Specifies the user name on the FTP/RCP server.
PASSWORD	Specifies the password for the user.
VRF-NAME	Specifies the name of the VRF instance which the TFTP/FTP/RCP server belongs to.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

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. Use this command to upload the system log to the TFTP server. 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 45421 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://10.1.1.254/switch-config.cfg...
 Transmission start...
 Transmission finished, file length 45421 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 "switch-config.cfg" file in the NVRAM immediately by using the increment method.

```
Switch# copy flash: switch-config.cfg running-config

Source filename [switch-config.cfg]?
Destination filename running-config? [y/n]:  y

 Executing script file switch-config.cfg ......
 Executing done

Switch#
```

This example shows how to download an image file from the TFTP server to all units in the stack.

```
Switch# copy tftp: //10.1.1.254/image.had flash: image.had

Address of remote host [10.1.1.254]?
Source filename [image.had]?
Destination filename [image.had]?
 Accessing tftp://10.1.1.254/image.had...
 Transmission start...
 Transmission finished, file length 8315060 bytes.
 Transmission to slave start.................   Done.
 Transmission to slave finished, file length 8315060 bytes.
 Please wait, programming flash.............. Done.
```

```
 Wait slave programming flash complete...
 Done.

Switch#
```

103-7 ip tftp source-interface

This command is used to specify the interface whose IP address will be used as the source address for initiating TFTP packets. To revert to the default setting, use the **no** form of this command.

ip tftp source-interface *INTERFACE-ID*

no ip tftp source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source address for initiating TFTP packets.

Default

The IP address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to specify the interface whose IP address will be used as the source address for initiating TFTP packets. To load the software from the out of band management port, specify the interface ID for the out of band management port.

Example

This example shows how to download software from the out of band management port.

```
Switch# configure terminal
Switch(config)# ip tftp source-interface mgmt0
Switch(config)#
```

103-8 ip ftp source-interface

This command is used to specify the interface whose IP address will be used as the source address for initiating FTP packets. To revert to the default setting, use the **no** form of this command.

ip ftp source-interface *INTERFACE-ID*

no ip ftp source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source address for initiating FTP packets.

Default

By default, the IP address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the interface whose IP address will be used as the source address for initiating FTP packets. To do software loading via the out of band management port, specify the interface ID for the out of band management port.

Example

This example shows how to do software download via the out of band management port.

```
Switch# configure terminal
Switch(config)# ip ftp source-interface mgmt0
Switch(config)#
```

103-9 ip rcp source-interface

This command is used to specify the interface whose IP address will be used as the source address for initiating RCP packets. To revert to the default setting, use the **no** form of this command.

ip rcp source-interface *INTERFACE-ID*

no ip rcp source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source address for initiating RCP packets.

Default

By default, the IP address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the interface whose IP address will be used as the source address for initiating RCP packets. To do software loading via the out of band management port, specify the interface ID for the out of band management port.

Example

This example shows how to do software download via the out of band management port.

```
Switch# configure terminal
Switch(config)# ip rcp source-interface mgmt0
Switch(config)#
```

103-10 show boot

This command is used to display the boot configuration file and the boot image setting.

show boot [unit *UNIT-ID***]**

Parameters

UNIT-ID	(Optional) Specifies the unit to be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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

Unit 1
Boot image: c:/bootimage.had
Boot config: c:/def_usr.cfg

Unit 2
Boot image: c:/bootimage.had
Boot config: c:/def_usr.cfg

Switch#
```

103-11 show running-config

This command is used to display the commands in the running configuration file.

show running-config [effective | all] [interface *INTERFACE-ID***]**

Parameters

effective	(Optional) Specifies to display command configurations that affect the behavior of the device. All other lower layer settings of STP are not displayed. The lower layer settings will only be displayed when the higher layer settings are enabled.
all	(Optional) Specifies to display all command configurations, including commands that corresponds to default parameters.
interface *INTERFACE-ID*	Specifies to display command configurations corresponding to the specified interface.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command displays 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 : 149304 bytes

#------------------------------------------------------------------------------
#                     DXS-3600-28SC Gigabit Ethernet Switch
#                               Configuration
#
#                           Firmware: Build 2.00.012
#           Copyright(C) 2013 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


# STACK

end
stack preempt
end

# DEVICE
configure terminal
end


# AAA

configure terminal
# AAA START
```

```
 no aaa new-model
# AAA END
end

# PRIVMGMT
configure terminal
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
# LOGIN START
# LOGIN END
                                    <Output Truncated>
```

103-12 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command displays 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-3600-28SC Gigabit Ethernet Switch
#                               Configuration
#
#                          Firmware: Build 2.00.012
#           Copyright(C) 2013 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


# STACK
```

```
end
stack preempt
end

# DEVICE
configure terminal
end


# AAA

configure terminal
# AAA START
 no aaa new-model
# AAA END
end

# PRIVMGMT
configure terminal
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
                                    <Output Truncated>
```

104. System Log Commands

104-1 clear logging

This command is used to delete log messages in the system logging buffer.

clear logging

Parameters

None.

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command deletes 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#
```

104-2 logging buffered

This command is used to enable logging of system messages to the local message buffer. Use the **no** 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, debugging.
discriminator	(Optional) Specifies to filter the message to be sent to local buffer based on the discriminator.
write-delay *SECONDS*	(Optional) Specifies to delay periodical writing of the logging buffer to the FLASH by the amount of seconds specified.

Default

By default, the severity level is warning (4).

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

104-3 logging console

This command is used to enable the logging of system messages to the local console. Use the **no** 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

	the local console. 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, debugging.
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.

Command Default Level

Level: 12.

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)#
```

104-4 logging discriminator

This command is used to create a discriminator that can be further used to filter SYSLOG messages sent to various destinations.

logging discriminator *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

no 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.

Command Default Level

Level: 12.

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)#
```

104-5 logging server

This command is used to create a SYSLOG server host to log the system messages or debug output. Use the **no** command to remove a SYSLOG server host.

logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***] [severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility** *FACILITY-TYPE***] [discriminator** *NAME***] [port** *UDP-PORT***]**

no logging server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***]**

Parameters

IP-ADDRESS	Specifies the IP address of the SYSLOG server host.
IPV6-ADDRESS	Specifies the IPv6 address of the log server host.
VRF-NAME	Specifies the name of the routing forwarding instance.
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, debugging.

FACILITY-TYPE	(Optional) Specifies the facility type as a decimal value from 0 to 23. If not specified, the default facility is local7 (23).
discriminator	(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.

Command Default Level

Level: 12.

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)#
```

104-6 logging smtp

This command is used to enable the logging of system messages to email recipients. Use the **no** command to disable the logging of messages to email recipients and revert to the default setting.

logging smtp [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

no logging smtp

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 email recipients. 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, debugging.
discriminator	(Optional) Specifies to filter the message to email recipients based on the discriminator.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The system messages can also be logged to email recipients. This command does not take effect if the specified discriminator does not exist. Thus the default setting of the command is applied. Messages must enter the local message buffer first before it can be further dispatched to email recipients.

Specify the severity level of the messages in order to restrict the system messages that are logged. The messages which are at the specified severity level or higher will be logged to the email recipients.

Example

This example shows how to enable the logging of system messages with a severity higher than warnings to email recipients.

```
Switch# configure terminal
```

```
Switch(config)# logging smtp severity warnings
Switch(config)#
```

104-7 logging source-interface

This command is used to specify the interface whose IP address will be used as the source address for sending the SYSLOG packet. To revert to default setting, use the **no** form of this command.

logging source-interface *INTERFACE-ID*

no logging source-interface

Parameters

INTERFACE-ID	Specifies the interface whose IP address will be used as the source address of the SYSLOG packet.

Default

By default, the IP address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the interface whose IP address will be used as the source address of the SYSLOG packet.

Example

This example shows how to configure VLAN 100 as the source interface for SYSLOG packets.

```
Switch# configure terminal
Switch(config)# logging source-interface vlan100
Switch(config)#
```

104-8 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 2013-01-02 16:37:36 EVN-5-FANINS Fan tray is inserted
#1 2013-01-02 16:35:54 IF-5-LINKDN port-channel10 is link down

Switch#
```

104-9 show attack-logging

This command is used to display attack log messages.

show attack-logging unit *UNIT-ID* **[index** *INDEX***]**

Parameters

UNIT-ID	Specifies the unit on which the attack log messages will be displayed.
INDEX	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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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 index 1
Attack log messages:
1  2013-10-17 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Switch#
```

104-10 clear attack-logging

This command is used to delete the attack log.

clear attack-logging {unit *UNIT-ID* **| all}**

Parameters

UNIT-ID	Specifies the unit on which the attack log messages will be cleared.
all	Specifies to clear all attack log entries.

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 12.

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#
```

105. Time and SNTP Commands

105-1 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, January, Jan, February, Feb, and so on).
YEAR	Specifies the current year (no abbreviation).

Default

None.

Command Mode

Privilege EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Generally, if the system is synchronized by a valid outside timing mechanism, such as SNTP, there is mp 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, 2013.

```
Switch# clock set 18:00:00 4 Jul 2013
Switch#
```

105-2 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, January, February, 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.

Command Default Level

Level: 12.

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 April 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 April 2:00 last sun October 2:00
Switch(config)#
```

105-3 clock timezone

This command is used to set the time zone for display purposes. To set the time to the Coordinated Universal Time (UTC), use the **no** form of this command.

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.

Command Default Level

Level: 12.

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 ahead of UTC.

```
Switch# configure terminal
Switch(config)# clock timezone - 8
Switch(config)#
```

105-4 show clock

This command is used to display the time and date information.

show clock

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

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  : SNTP
Current Time         : 18:20:04, 2013-07-04
Time Zone            : UTC +02:30
Daylight Saving Time : Recurring
Offset in Minutes    : 30
    Recurring From   : Apr 2nd Tue 15:00
              To     : Oct 2nd Wed 15:30

Switch#
```

105-5 show sntp

This command is used to display information about the SNTP server.

show sntp

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display information about the SNTP server.

Example

This example shows how to display SNTP information.

```
Switch# show sntp

SNTP Status         :Enabled
SNTP Pool Interval  : 720 seconds

SNTP Server Status:

SNTP Server                                    Stratum Version Last Receive
---------------------------------------------- ------- ------- ---------------
10.0.0.11                                      8       4       00:02:02
10.0.0.11(VRF test)                            7       4       00:01:02 Synced
10::2                                          ------- ------- ---------------
FE80::1111vlan1                                ------- ------- ---------------
---------------------------------------------- ------- ------- ---------------

Total Entries:4
```

```
Switch#
```

105-6 sntp server

This command is used to allow the system clock to be synchronized with an SNTP time server. To remove a server from the list of SNTP servers, use the **no** form of this command.

sntp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***]**

no sntp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [vrf** *VRF-NAME***]**

Parameters

IP-ADDRESS	Specifies the IP address of the time server which provides the clock synchronization.
IPV6-ADDRESS	Specifies the IPv6 address of the time server.
VRF-NAME	Specifies the name of the routing forwarding instance.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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.

Enter this command once for each NTP server. Configure the system with either this command or the **sntp broadcast client global configuration** command in order to enable SNTP. Create multiple SNTP servers by enter this command multiple times with different SNTP server IP addresses.

Use the **no** 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)#
```

105-7 sntp enable

This command is used to enable the SNTP function. Use the **n**o 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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

105-8 sntp interval

This command is used to set the interval for the SNTP client to synchronize its clock with the server.

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.

Command Default Level

Level: 12.

Usage Guideline

This command is used 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)#
```

106. Time Range Commands

106-1 periodic

This command is used to specify the period of time for a time range profile. This command is used in the time-range configuration mode.

periodic {daily *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

no periodic {daily *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

Parameters

daily *HH:MM* **to** *HH: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.

Command Default Level

Level: 12.

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)#
```

106-2 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

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

If the name is not 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#
```

106-3 time-range

This command is used to enter the time range configuration mode to define a time range. Use the **no** 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.

Command Default Level

Level: 12.

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)#
```

107. Traffic Segmentation Commands

107-1 show traffic-segmentation forward

This command is used to display the traffic segmentation for some ports or all ports.

show traffic-segmentation forward [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies ID of an interface. The acceptable interface will be physical port or port channel.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

While entering this command without any other keywords, the traffic segmentation configuration for all ports is displayed. Otherwise, only the specified interface's traffic segmentation is displayed.

Example

This example shows how to display the configuration of traffic segmentation for eth3/0/1.

```
Switch# show traffic-segmentation forward interface eth3/0/1

Interface        Forwarding Domain
------------ ----------------------------------------
eth1/0/1        eth1/0/1, eth1/0/4, eth1/0/5, eth1/0/6

Total Entries: 1

Switch#
```

107-2 traffic-segmentation forward

This command is used to restrict the Layer 2 packet forwarding domain of packets received by the configured port. Use **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 ID of an interface allowed. The allowed interfaces include physical port.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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 command will 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, then there is no restriction on Layer 2 forwarding of packets received by the port.

Example

This example shows how to configure traffic segmentation. It restricts the flooding domain of eth3/0/1 to a set of ports, which are eth4/0/1 – eth4/0/6.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# traffic-segmentation forward interface range eth4/0/1-6
Switch(config-if)#
```

108. Unicast Reverse Path Forwarding (URPF) Commands

108-1 ip urpf

This command is used to enable Unicast Reverse Path Forwarding (URPF) checking globally. Use the **no** form of this command to disable the global state of URPF.

ip urpf

no ip urpf

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

One common method to initiate an attack is to utilize IPv4/IPv6 source address spoofing. When using this method, a hacker attempts to send traffic into the network with a source address that is known or trusted by the target. If no protection exists, the organizational network will allow the traffic and potentially be open to a number of different attack types. URPF helps to mitigate problems caused by malformed or forged IPv4/IPv6 source addresses passing through a router.

The **ip urpf global configuration** command is used to enable URPF globally and the **ip verify unicast source interface mode** command is used to enable URPF on the interface. To enable URPF on an interface, enable the function both globally and on the interface.

Example

This example shows how to enable the URPF checking globally.

```
Switch# configure terminal
Switch(config)# ip urpf
WARNING: The command does not take effect until after the next reboot.
Switch(config)#
```

108-2 ip verify unicast source

This command is used to configure URPF on interfaces. Use the **no** form of this command to disable URPF checking on an interface or to revert the settings to the default.

ip verify unicast source [reachable-via {any | rx}] [allow-default] [access-group *IP-ACCESS-LIST-NAME***] [ipv6-access-group** *IPV6-ACCESS-LIST-NAME***]**

no ip verify unicast source [reachable-via] [allow-default] [access-group] [ipv6-access-group]

Parameters

reachable-via	(Optional) Specifies the mode how URPF examines the incoming packets.
any	Specifies to verify if the source address is present in the routing table (sometimes referred to as the loose mode).
rx	Specifies to verify if the source address is present in the routing table and the incoming interface matches the source and is reachable through the interface on which the packet was received (sometimes referred to as the strict mode). This is the default option.
allow-default	(Optional) Specifies allowing the use of the default route for URPF verification.
access-group *IP-ACCESS-LIST-NAME*	(Optional) Specifies the name of the IPv4 ACL to be checked.
ipv6-access-group *IPV6-ACCESS-LIST-NAME*	(Optional) Specifies the name of the IPV6 ACL to be checked.

Default

By default, URPF checking is not performed.

By default, the checking mode is RX.

By default, no IPv4/IPv6 access list is specified.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Unicast RPF helps to mitigate problems caused by the introduction of malformed or forged IPv4/IPv6 source addresses into a network by discarding IPv4/IPv6 packets that lack a verifiable IPv4/IPv6 source address.

When Unicast RPF is effectively enabled on an interface, the switch examines all IPv4 and IPv6 packets received as input on that interface to make sure that the source address and source interface appear in the routing table and match the interface on which the packet was received.

The reverse path checking will not be performed in the following situations:

- The destination IPv4/IPv6 address is not a unicast address.
- The source IP address is an IPv6 address and the address is a link-local address.
- The received packet is a BOOTP/DHCP packet (the source IP is 0.0.0.0 and destination IP is 255.255.255.255).

Example

This example shows how to enable Unicast RPF checking on interface eth0/8.

```
Switch# configure terminal
Switch(config)# interface eth0/8
Switch(config-if)# ip verify unicast source
Switch(config-if)#
```

This example shows how to configure the Unicast RPF checking mode to any and allow the use of the default route for RPF verification on interface eth0/1.

```
Switch# configure terminal
Switch(config)# interface eth0/1
Switch(config-if)# ip verify unicast source  reachable-via any allow-default
Switch(config-if)#
```

This example shows how to configure the IP ACL, named “v4isp” and IPv6 ACL, named “v6isp” for Unicast RPF checking on interface eth0/8.

```
Switch# configure terminal
Switch(config)# interface eth0/8
Switch(config-if)# ip verify unicast source access-group v4isp ipv6-access-group v6isp
Switch(config-if)#
```

108-3 show ip urpf

This command is used to display the URPF settings.

show ip urpf [*INTERFACE-ID* **[, | -]]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface to display. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the current settings of URPF. If this command is issued without an interface ID, only the global Unicast RPF settings will be displayed.

Example

This example shows how to displays the settings of URPF on interfaces eth1/0/1-3.

```
Switch# show ip urpf 1/0/1-3

URPF Global State : Enabled (Save And Reboot Required)

Port#       State       Reachable-   Allow-     IP Access List Name
                        Via          Default    IPv6 Access List Name
----------  --------  ----------  ---------  --------------------------------
```

```
1/0/1          Enabled      Any        True         v4gateway
                                                    v6gateway
1/0/2          Disabled     rx         False
                                                    v6Acl1
1/0/3          Enabled      rx         True         v4Acl2

Switch#
```

Display Parameters

URPF Global State	The global state of Unicast RPF checking.
Save And Reboot Required	Indicates that the configured Unicast RPF global state does not take effect until after the next reboot.
State	The state of Unicast RPF.
Port	The port number.
Reachable-Via	The mode how Unicast RPF examines the incoming packets.
Allow-Default	Indicates whether allows the use of the default route for RPF verification.
IP Access List Name	Indicates the name of the IP ACL to be checked. The empty string indicates the IP Access List Name is not specified.
IPv6 Access List Name	Indicates the name of the IPv6 ACL to be checked. The empty string indicates the IPv6 Access List Name is not specified.

109. Virtual LAN (VLAN) Tunnel Commands

109-1 dot1q inner ethertype

This command is used to specify the system's inner TPID. Use the **no** command to revert the setting to default.

dot1q inner ethertype *VALUE*

no dot1q inner ethertype

Parameters

VALUE	Specifies the system's inner TPID. The value is in the hexadecimal form. The range is 0x1 to 0xFFFF.

Default

The default inner TPID is 0x8100.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to configure the inner TPID of the system. The inner TPID is used to decide if the ingress packet is C-tagged. The Inner TPID is per system configurable.

Example

This example shows how to configure the inner TPID to 0x9100.

```
Switch# configure terminal
Switch(config)# dot1q inner ethertype 0x9100
Switch(config)#
```

109-2 dot1q tunneling ethertype

This command is used to specify the outer TPID for the service VLAN tag. Use the **no** command to restore the setting back to default setting.

dot1q tunneling ethertype *VALUE*

no dot1q tunneling ethertype

Parameters

VALUE	Specifies the outer TPID for the service VLAN tag. The value is in the hexadecimal form. The range is 0x1 to 0xFFFF.

Default

By default, this option is 0x8100.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

An 802.1Q tunnel port behaves as an UNI port of a service VLAN. The trunk ports which are tagged members of the service VLAN behave as the NNI ports of the service VLAN.

Only configure the 802.1Q tunneling Ethernet type on ports that are connected to the provider bridge network, which receives and transmits the service VLAN tagged frames. If the tunnel Ethernet type is configured, the specified value will be the TPID in the outer VLAN tag of the transmitted frames out of this port. The specified TPID is also used to identify the service VLAN tag for the received frame on this port.

Example

This example shows how to configure the 802.1Q tunneling TPID on interface Ethernet1/0/1 to 0x88a8.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# dot1q tunneling ethertype 0x88a8
Switch(config-if)#
```

109-3 switchport mode dot1q-tunnel

This command is used to specify the switch port to operate as a dot1q tunnel port.

switchport mode dot1q-tunnel

Parameters

None.

Default

By default, the switch port is operated as a hybrid port.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to specify the switch port to operate as a dot1q tunnel port.

Example

This example shows how to specify the switch port to operate as a dot1q tunnel port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport access vlan 100
```

```
Switch(config-if)#
```

109-4 switchport vlan mapping

This command is used to specify the VLAN translation entry for a trunk port or to specify the service VLAN mapping entry for a dot1q tunnel port. Use the **no** command to remove the VLAN translation entry or the service VLAN mapping entry.

switchport vlan mapping original-vlan *ORIGINAL-VLAN* **[, | -] {[***ORIGINAL-INNER-VLAN***] resultant–vlan** *RESULTANT-VLAN* **[***RESULTANT-INNER-VLAN***] | dot1q-tunnel** *DOT1Q-TUNNEL-VLAN***} [priority** *COS-VALUE***]**

no switchport vlan mapping original-vlan *ORIGINAL-VLAN* **[, | -] [***ORIGINAL-INNER-VLAN***]**

Parameters

ORIGINAL-VLAN	Specifies the original VLAN ID that will be matched for incoming packets. The range is from 1 to 4094.
ORIGINAL-INNER-VLAN	(Optional) Specifies that the original inner VLAN is used to match the inner VID for incoming packets on the trunk mode port. The range is from 1 to 4094.
RESULTANT-VLAN	Specifies the translated service VLAN ID. The range is from 1 to 4094. The service VLAN will replace the original VLAN for matched packets.
RESULTANT-INNER-VLAN	(Optional) Specifies the new inner VLAN that will replace original inner VLAN on trunk mode port.
DOT1Q-TUNNEL-VLAN	Specifies the service VLAN ID that will be added for matched packets on the dot1q-tunnel mode port.
COS-VALUE	(Optional) Specifies the priority for the rule. If not specified, the priority of the service VLAN tag will be set to 0.
,	(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 and after the hyphen.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command only takes effect for the port or port-channel that is set to 802.1Q tunnel mode or trunk mode.

If the **dot1q-tunnel** parameter is specified in this command, once the C-VLAN tag of the incoming packet matches the specified original VLAN, the specified S-VLAN is added to make the packet becomes double tagged. Specify a VLAN range to map multiple original VLANs to single S-VLAN. This rule can be configured on an 802.1Q tunnel port. Otherwise, the rule will not take effect (its status is inactive).

If the *RESULTANT-VLAN* parameter is specified in this command, the rule performs VLAN translation. Once the VLAN tag of the incoming packet matches the specified original VLAN, the specified S-VLAN replaces original VLAN. The VLAN translation is one-to-one mapping, i.e. you cannot configure multiple original VLANs map to single S-VLAN. The VLAN translation can be configured on both 802.1q tunnel or trunk port.

Optional, configure a 2:1 VLAN translation rule by specifying the *ORIGINAL-INNER-VLAN* parameter. In this case, the outer and inner tag of the incoming packets is used to match the VLAN translation rule. The outer VLAN of the matched packet is replaced by translated service VLAN and the original inner VLAN is not modified.

Configure a 2:2 VLAN translation rule by specifying the *RESULTANT-INNER-VLAN* parameter. In this case, the original inner VLAN of the matched packet will be replaced by the specified new inner VLAN.

Usually, the 2:1 and 2:2 VLAN translations are configured on trunk ports.

When VLAN mapping entries are configured on a trunk port, the packet handling behavior is different from an ordinary trunk port. When a packet arrives at the port, its VLAN is translated to a new VLAN. Then, the learning and subsequent operations are based on the translated VLAN. For packets egress from the port, the VLAN of the packet will be translated back to the original VLAN before the packet is transmitted.

When configuring VLAN mapping entries to translate an original VLAN to an S-VLAN, the user cannot configure another VLAN mapping entry to translate other original VLANs to the S-VLAN or configure the VLAN mapping rule bundling C-VLANs to the S-VLAN, and vice versa.

If there is no VLAN mapping entry or rule that matches the incoming tagged packet and the VLAN mapping miss drop option is enabled on the port, the packet will be dropped. If the VLAN mapping miss drop option is disabled, the port-based service VLAN will be assigned for the unmatched packet.

Example

This example shows how to configure VLAN mapping entries for a trunk port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)# switchport vlan mapping original-vlan 100 resultant–vlan 1100
Switch(config-if)# switchport vlan mapping original-vlan 200 resultant–vlan 1200
Switch(config-if)#
```

This example shows how to configure VLAN mapping entries for an 802.1Q tunnel port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/2
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# switchport vlan mapping original-vlan 600 resultant–vlan 1600
Switch(config-if)# switchport vlan mapping original-vlan 700 dot1q-tunnel 1700
Switch(config-if)# switchport access vlan 1600
Switch(config-if)# switchport hybrid allow vlan add  untagged 1700
Switch(config-if)#
```

109-5 dot1q-tunnel insert dot1q-tag

This command is used to specify the dot1q VLAN tag insertion. Use the **no** command to remove the dot1q VLAN tag insertion.

dot1q-tunnel insert dot1q-tag *DOT1Q-VLAN*

no dot1q-tunnel insert dot1q-tag

Parameters

DOT1Q-VLAN	Specifies the dot1q VLAN ID that is inserted to the untagged packets which are received on the dot1q tunnel port.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If this command is configured, when the untagged packets are received on the 802.1Q tunnel port, the specified dot1q VLAN tag will be inserted into it as inner tag.

Example

This example shows how to configure an interface port 1 to insert the inner tag with VLAN 10.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# dot1q-tunnel insert dot1q-tag 10
Switch(config-if)#
```

109-6 vlan mapping miss drop

This command is used to enable the dropping of VLAN mapping unmatched packets. Use the **no** command to disable the VLAN mapping miss dropping.

vlan mapping miss drop

no vlan mapping miss drop

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port and port-channel interfaces that are set to 802.1Q tunnel mode. If the VLAN mapping miss dropping option is enabled on the receiving port, when the original

VLAN of the received packets cannot match the VLAN mapping entries or rules on this port, the received packets will be dropped.

Example

This example shows how to configure an interface port 1 to enable VLAN mapping miss dropping.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# vlan mapping miss drop
Switch(config-if)#
```

109-7 dot1q-tunnel trust inner-priority

This command is used to set the trusting dot1q priority. Use the **no** command to remove the setting.

dot1q-tunnel trust inner-priority

no dot1q-tunnel trust inner-priority

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the trusting dot1q priority option, on a dot1q tunnel port, is enabled the priority of the dot1q VLAN tag in the received packets will be copied to the service VLAN tag.

Example

This example shows how to configure the interface port 1 to trust inner priority.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode dot1q-tunnel
Switch(config-if)# dot1q-tunnel trust inner-priority
Switch(config-if)#
```

109-8 vlan mapping profile

This command is used to create a VLAN mapping profile or enter the VLAN mapping profile configuration mode. Use the **no** command to remove the VLAN mapping profile.

vlan mapping profile *ID* **[type [ethernet] [ip] [ipv6]]**

no vlan mapping profile *ID*

Parameters

ID	Specifies the ID of the VLAN mapping profile. A lower ID has a higher priority. The ID range is from 1 to 1000.
type	Specifies the profile types. Different profiles can match different fields. **ethernet:** The profile can match Layer 2 fields. **ip:** The profile can match Layer 3 IP fields. **ipv6:** The profile can match IPv6 destination or source addresses.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A VLAN mapping profile can be used to provide flexible and powerful flow-based VLAN translation. For creating a VLAN mapping profile, users must specify the type to decide which fields can be matched by the profile rules.

Example

This example shows how to create a VLAN mapping profile for matching Ethernet fields.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ethernet
Switch(config-vlan-map)#
```

109-9 vlan mapping rule

This command is used to configure the VLAN mapping rules of the profile. Use the **no** command to remove the previous configured rules.

rule [*SN***] match [src-mac** *MAC-ADDRESS***] [dst-mac** *MAC-ADDRESS***] [priority** *COS-VALUE***] [inner-vid** *VLAN-ID***] [ether-type** *VALUE***] [src-ip** *NETWORK-PREFIX***] [dst-ip** *NETWORK-PREFIX***] [src-ipv6** *IPV6-NETWORK-PREFIXIPREFIX-LENGTH***] [dst-ipv6** *IPV6-NETWORK-PREFIXIPREFIX-LENGTH***] [dscp** *VALUE***] [src-port** *VALUE***] [dst-port** *VALUE***] [ip-protocol** *VALUE***] {dot1q-tunnel | translate} outer-vid** *VLAN-ID* **[priority** *COS-VALUE***] [inner-vid** *VLAN-ID***]**

no rule *SN* **[- | ,]**

Parameters

SN	(Optional) Specifies the sequence number of the VFP rule. If not specified, the SN begins from 10 and the increment is 10. The SN range is from 1 to 10000
src-mac *MAC-ADDRESS*	Specifies the source MAC address.

dst-mac *MAC-ADDRESS*	Specifies the destination MAC address.
priority *COS-VALUE*	Specifies the 802.1p priority.
inner-vid *VLAN-ID*	Specifies the inner VLAN ID.
ether-type *VALUE*	Specifies the Ethernet type.
src-ip *NETWORK-PREFIX*	Specifies the source IPv4 address.
dst-ip *NETWORK-PREFIX*	Specifies the destination IPv4 address.
src-ipv6 *IPV6-NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the source IPv6 address.
dst-ipv6 *IPV6-NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the destination IPv6 address.
dscp *VALUE*	Specifies the DSCP value.
src-port *VALUE*	Specifies the source TCP/UDP port number.
dst-port *VALUE*	Specifies the destination TCP/UDP port number.
ip-protocol *VALUE*	Specifies the Layer 3 protocol value.
dot1q-tunnel	Specifies that the outer-VID will be added for matched packets.
translate	Specifies that the outer-VID will replace the outer-VID of the matched packets.
outer-vid *VLAN-ID*	Specifies the new outer VLAN ID.
priority *COS-VALUE*	(Optional) Specifies the 802.1p priority in the new outer TAG. If not specified, the priority of the new outer tag is 0.
inner-vid *VLAN-ID*	(Optional) Specifies the new inner VLAN ID.

Default

None.

Command Mode

VLAN Mapping Profile Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The rule command is used to configure the VLAN mapping rules of the profile. If a profile is applied on an interface, the switch matches the incoming packets according to the rules of the profile. If the packets match a rule, the action of the rule will be taken. The action may be adding or replacing the outer-VID. Optionally, specify the priority of the new outer-TAG or specify the packets new inner-VID.

The match order depends on the rule's sequence number of the profile and stopped when first matched. If the sequence number is not specified, it will be allocated automatically. The sequence number begins from 10 and the increment is 10. Multiple different types of profiles could be configured onto one interface.

Example

This example shows how to configure rules for VLAN mapping profile 1.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)#
```

109-10 switchport vlan mapping profile

This command is used to apply the VLAN mapping rules of a profile to the specified interface. Use the **no** form of the command to remove the association.

switchport vlan mapping profile *PROFILE-ID*

no switchport vlan mapping profile *PROFILE-ID*

Parameters

PROFILE-ID	(Optional) Specifies the ID of the VLAN mapping profile.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to apply the VLAN mapping profile to the specified interface. The interface can be a physical port or a port-channel interface which is set to the dot1q tunnel mode.

If a profile is applied on an interface, the switch tests the incoming packets according to the rules of the profile. If the packets match a rule, the action of the rule will be taken.

Setting the port to a mode other than the dot1q-tunnel mode will lead to the VLAN mapping profile configuration to be removed.

Example

This example shows how to configure a VLAN mapping profile and apply it to the 802.1Q tunnel port 1. The customer packets that come from 100.1.1.0/24 will be added to S-VLAN 100 and the packets that go to 200.1.1.0/24 will be added to S-VLAN 200.

```
Switch# configure terminal
Switch(config)# vlan mapping profile 1 type ip
Switch(config-vlan-map)# rule 10 match src-ip 100.1.1.0/24 dot1q-tunnel outer-vid 100
Switch(config-vlan-map)# rule 20 match dst-ip 200.1.1.0/24 dot1q-tunnel outer-vid 200
Switch(config-vlan-map)# exit
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport vlan mapping profile 1
Switch(config-if)#
```

109-11 show dot1q ethertype

This command is used to display TPID settings.

show dot1q ethertype [*INTERFACE-ID* **[- | ,]]**

Parameters

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

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the service VLAN tag Ethernet type.

Example

This example shows how to display the 802.1Q TPID setting for all interfaces.

```
Switch#show dot1q ethertype

802.1q inner Ethernet Type is 0x8100
eth1/0/1
802.1q tunneling Ethernet Type is 0x88a8
eth1/0/2
802.1q tunneling Ethernet Type is 0x88a8

Switch#
```

109-12 show dot1q-tunnel

This command is used to display the dot1q VLAN tunneling configuration on interfaces.

show dot1q-tunnel [interface *INTERFACE-ID* **[, | -]]**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces that will be displayed. If not specified, display all 802.1Q tunnel ports.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the 802.1Q tunneling configuration on interfaces.

Example

This example shows how to display all 802.1Q tunnel ports configuration.

```
Switch# show dot1q-tunnel

dot1q Tunnel Interface: eth1/0/1
Trust inner priority       : Enabled
  VLAN mapping miss drop    : Disabled
  VLAN mapping profiles      : 1, 2, 3

dot1q Tunnel Interface: eth1/0/2
Trust inner priority       : Disabled
VLAN mapping miss drop    : Enabled
Insert dot1q tag           : VLAN 10

Switch#
```

109-13 show vlan mapping

This command is used to display the VLAN mapping configuration.

show vlan mapping [interface *INTERFACE-ID* **[, | -]]**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces that will be displayed. If not specified, display the all VLAN mappings.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display VLAN mapping configurations.

Example

This example shows how to display all VLAN mappings.

```
Switch# show vlan mapping

Interface  Original VLAN  Translated VLAN  Priority  Status
---------  -------------  ---------------  --------  --------
eth1/0/1     1              dot1q-tunnel 10  0           Active
eth1/0/1     2              dot1q-tunnel 11  5           Active
eth1/0/2     10             Translate 100     0          Active
eth1/0/2     20             Translate 200     0          Active
eth1/0/3     30/3           Translate 300     0         Active
eth1/0/3     40/1           Translate 400/2   2         Active

Total entries: 6

Switch#
```

109-14 show vlan mapping profile

This command is used to display the configured VLAN mapping profile information.

show vlan mapping profile [*ID*]

Parameters

ID	(Optional) Specifies the ID of the VLAN mapping profile. If not specifies, display all configured VLAN mapping profiles.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display configured VLAN mapping profile information.

Example

This example shows how to display all VLAN mapping profile information.

```
Switch# show vlan mapping profile

VLAN mapping profile:1  type:ip
rule 10 match src-ip 100.1.1.0/24, action dot1q-tunnel outer-vid 100, priority 0
rule 20 match dst-ip 200.1.1.0/24, action dot1q-tunnel outer-vid 200, priority 1
```

```
rule 30 match src-ip 192.1.1.0/24, action dot1q-tunnel outer-vid 300, priority 0
Total Entries: 3
VLAN mapping profile:2  type:ethernet
rule 10 match src-mac 00-00-00-00-00-01,action translate outer-vid 40, priority 2
rule 20 match inner-vid 5, action translate outer-vid 10, priority 0
Total Entries: 2

Switch#
```

110. Virtual LAN (VLAN) Commands

110-1 acceptable-frame

This command is used to set the acceptable types of frames by a port. Use the **no** form of the command to reset to the default setting.

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.

Command Default Level

Level: 12.

Usage Guideline

This command is used to set the acceptable types of frames by a port.

Example

This example shows how to set the acceptable frame type to **tagged-only** for port eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# acceptable-frame tagged-only
Switch(config-if)#
```

110-2 ingress-checking

This command is used to enable ingress checking for frames received by a port. Use the **no** 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.

Command Default Level

Level: 12.

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 set ingress checking to enabled port eth1/0/1.

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

110-3 mac-vlan

This command is used to create the MAC-based VLAN classification entry. Use the **no** form of this command to remove the MAC-based VLAN classification entry.

mac-vlan *MAC-ADDRESS* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

no mac-vlan *MAC-ADDRESS*

Parameters

MAC-ADDRESS	Specifies the MAC address for the entry.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If not specified, the default CoS is 0.
VLAN-ID	Specifies the VLAN ID for the MAC-based VLAN entry.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create the MAC-based VLAN classification entry. The classification entry will be applied to packets received by the switch. By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN.

Example

This example shows how to create a MAC-based VLAN ID entry for the MAC address 00-80-cc-00-00-11.

```
Switch# configure terminal
Switch(config)# mac-vlan 00-80-cc-00-00-11 vlan 101 priority 4
Switch(config)#
```

110-4 protocol-vlan profile

This command is used to create a protocol group. Use the **no** command to remove the specified protocol group.

protocol-vlan profile *PROFILE-ID* **frame-type {ethernet2 | snap | llc} ether-type** *TYPE-VALUE*

no protocol-vlan profile *PROFILE-ID*

Parameters

PROFILE-ID	Specifies the protocol group to add or delete.
frame-type	Specifies the frame type.
ethernet2	Specifies the value for the type of the Ethernet II frames.
snap	Specifies the value for the type of the SNAP frames.
llc	Specifies the value for the type of the LLC frames.
ether-type *TYPE-VALUE*	Specifies the type. This value should be 2 bytes in hexadecimal form.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **protocol-vlan profile** command in the global configuration mode to create a protocol group. Then use the **protocol-vlan profile** command in the interface configuration mode to configure the VLAN classification for the protocol group received by the port.

Example

This example shows how to create a protocol VLAN group with a group ID of 10, specifying that the IPv6 protocol (frame type is ethernet2 value is 0x86dd) will be used.

```
Switch# configure terminal
Switch(config)# protocol-vlan profile 10 frame-type ethernet2 ether-type 0x86dd
Switch(config)#
```

110-5 protocol-vlan profile (interface)

This command is used to configure the VLAN classification entry for a protocol group on a port. Use the **no** form of the command to remove the VLAN classification entry on a port.

protocol-vlan profile *PROFILE-ID* **vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

no protocol-vlan profile *PROFILE-ID*

Parameters

PROFILE-ID	Specifies the ID of the protocol group to be classified.
VLAN-ID	Specifies the VLAN ID of the protocol VLAN. Only one VLAN ID can be specified for each binding group.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If not specified, the default COS is 0.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this to specify a VLAN for a protocol group on a port. As a result, the packet received by the port that matches the specified protocol group will be classified to the specified VLAN. The VLAN does not need to exist to configure the command. The precedence for classifying the untagged packet is MAC-based > Subnet-based > Protocol VLAN.

Example

This example shows how to create a VLAN classification entry on eth1/0/1 to classify packets in the protocol group 10 to VLAN 3000.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# protocol-vlan profile 10 vlan 3000
Switch(config-if)#
```

110-6 subnet-vlan

The **subnet-vlan ipv4** command is used to configure a VLAN classification entry for an IPv4 subnet. The **subnet-vlan ipv6** command is used to configure a VLAN classification entry for an IPv6 subnet. Use the **no** form of this command to remove a subnet-based VLAN classification entry.

subnet-vlan {ipv4 *NETWORK-PREFIX NETWORK-MASK* **| ipv6** *IPV6-NETWORK-PREFIXIPREFIX-LENGTH***} vlan** *VLAN-ID* **[priority** *COS-VALUE***]**

no subnet-vlan {ipv4 *NETWORK-PREFIX NETWORK-MASK* **| ipv6** *IPV6-NETWORK-PREFIXIPREFIX-LENGTH***}**

Parameters

ipv4 *NETWORK-PREFIX*	Specifies the IPv4 network prefix and network mask.

NETWORK-MASK	
ipv6 *IPV6-NETWORK-PREFIXIPREFIX-LENGTH*	Specifies the IPv6 network prefix and the prefix length. The prefix length of IPv6 network address cannot be greater than 64 bits.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If not specified, the default COS is 0.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **subnet-vlan ipv4** command to configure a VLAN classification entry for an IPv4 subnet. Use the **subnet-vlan ipv6** command to configure a VLAN classification entry for an IPv6 subnet. The classification entry will be applied to packets received by the switch. By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN.

Example

This example shows how to configure VLAN classification entries to classify that packets belong to subnets 20.0.0.0/8, 192.0.0.0/8, and 3ffe:22:33:44::/64 to VLAN 100.

```
Switch# configure terminal
Switch(config)# subnet-vlan ipv4 20.0.0.0/8 vlan 100 vlan 100
Switch(config)# subnet-vlan ipv4 192.0.0.0/8 vlan 100 priority 4
Switch(config)# subnet-vlan ipv6 3ffe:22:33:44::/64 vlan 100
Switch(config)#
```

110-7 show protocol-vlan profile

This command is used to display the configuration settings of the protocol VLAN related setting.

show protocol-vlan {profile [*PROFILE-ID* **[, | -]] | interface [***INTERFACE-ID* **[, | -]]}**

Parameters

PROFILE-ID	(Optional) Specifies the protocol group to be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the port to display the protocol VLAN classification setting.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is required before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is required before or after the hyphen.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the settings for VLAN classification on a port based on the protocol group.

Example

This example shows how to display the setting for VLAN classification based on the protocol group on a port eth1/0/1 to eth1/0/3.

```
Switch# show protocol-vlan interface eth1/0/1-3

Interface    Protocol Group ID     VLAN    Priority
------------ -------------------- ------- ---------
eth1/0/1     1                    1       5
eth1/0/2     10                   3       0
             11                   2001    4
             12                   3002    1
eth1/0/3     2                    100     6

Switch#
```

This example shows how to display the protocol group profile settings.

```
Switch# show protocol-vlan profile

 Profile ID  Frame-type   Ether-type
 ----------  -----------  ----------------
 1           Ethernet2    0x86DD(IPv6)
 2           Ethernet2    0x0800(IP)
 3           Ethernet2    0x0806(ARP)

Total Entries: 3

Switch#
```

110-8 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* **[, | -]] | mac-vlan | subnet-vlan]**

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.
interface *INTERFACE-ID*	(Optional) Specifies the port to display the VLAN related setting.

,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space before and after the comma.
-	(Optional) Specifies a range of interfaces. No space before and after the hyphen.
mac-vlan	(Optional) Specifies to display MAC-based VLAN information.
subnet-vlan	(Optional) Specifies to display subnet-based VLAN information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used 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
   Tagged Member Ports   :
   Untagged Member Ports : 1/0/1-1/0/8

Total Entries : 1

Switch#
```

This example shows how to display the PVID, ingress checking, and acceptable frame type information for ports eth1/0/1-1/0/4.

```
Switch# show vlan interface eth1/0/1-1/0/4

eth1/0/1
VLAN mode              : Trunk
Native VLAN            : 5 (Untagged)
Trunk allowed VLAN     : 2,4,5,6
Ingress checking       : Enabled
Acceptable frame type  : Admit-all
Dynamic Tagged VLAN    : 100

eth1/0/2
VLAN mode              : Access
Access VLAN            : 2
Ingress checking       : Enabled
Acceptable frame type  : Untagged-only

eth1/0/3
```

```
VLAN mode              : Hybrid
Native VLAN            : 5
Hybrid untagged VLAN   : 2,4,5,6
Hybrid tagged VLAN     : 8,9,10
Ingress checking       : Enabled
Acceptable frame type  : Admit-All
Dynamic tagged VLAN    :
VLAN Precedence        : MAC-VLAN

eth1/0/4
VLAN mode              : Dot1q-tunnel
Access VLAN            : 800
Hybrid untagged VLAN   : 200, 600
Ingress checking       : Enabled
Acceptable frame type  : Admit-all
VLAN Precedence        : MAC-VLAN

Switch#
```

This example shows how to display all the MAC–based VLAN entries.

```
Switch# show vlan mac-vlan

MAC Address         VLAN ID   Priority  Status
 ------------------  --------  --------  ----------
 00-80-cc-00-00-11   101         4       Active
 00-11-22-00-00-05   200         5       Active

Total Entries: 2

Switch#
```

This example shows how to display all the subnet–based VLAN entries.

```
Switch# show vlan subnet-vlan

 Subnet                    VLAN ID  Priority
 ------------------------  -------  ---------
 20.0.0.0/8                100      0
 192.0.0.0/8               100      4
 3FFE:22:33:44::/64        100      0

Total Entries: 3

Switch#
```

110-9 switchport access vlan

This command is used to specify the access VLAN for an interface. Use the **no** form of the command to reset to the default setting.

switchport access vlan *VLAN-ID*

no switchport access vlan

Parameters

access vlan *VLAN-ID*	Specifies the access VLAN of the interface.

Default

By default, this access VLAN is VLAN 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command takes effect when the interface is set to access mode, or dot1q-tunnel 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 the interface 1/0/1 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)#
```

110-10 switchport hybrid allowed vlan

This command is used to specify the tagged or untagged VLANs for a hybrid port. Use the **no** form of the command to reset to the default setting.

switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* **[, | -]**

no switchport hybrid allowed vlan

Parameters

add	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 required before and after the comma.

-	(Optional) Specifies a range of VLANs. No space is required before and after the hyphen.

Default

By default, a hybrid port is an untagged member port of VLAN 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 interface eth1/0/1 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)#
```

110-11 switchport hybrid native vlan

This command is used to specify the native VLAN ID of a hybrid port. Use the **no** command to reset the native VLAN to the default setting.

switchport hybrid native vlan *VLAN-ID*

no switchport hybrid native vlan

Parameters

vlan *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.

Command Default Level

Level: 12.

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 interface eth1/0/1 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)#
```

110-12 switchport mode

This command is used to specify the VLAN mode for the port. Use the **no** command to reset the VLAN mode to the default setting.

switchport mode {access | hybrid | trunk | dot1q-tunnel}

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.
dot1q-tunnel	Specifies the port as a dot1q-tunnel port.

Default

By default, this option is **hybrid**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 all VLANs configured. The purpose of this VLAN mode is to support of protocol VLAN, subnet-based VLAN, and MAC-based VLAN.

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 a port is set to dot1q-tunnnel mode, the port behaves as an UNI port of a service VLAN.

When the switch-port mode is changed, the VLAN related setting associated with previous mode will be lost.

Example

This example shows how to set the interface eth1/0/1 as a trunk port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

110-13 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** command to reset 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	Specifies to add the specified VLAN list to the allowed VLAN list.
remove	Specifies to remove the specified VLAN list from the allowed VLAN list.
except	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 required before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is required before and after the hyphen.

Default

By default, all VLANs are allowed.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

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 interface eth1/0/1 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)#
```

110-14 switchport trunk native vlan

This command is used to specify the native VLAN ID of a trunk mode interface. Use the **no** interface command to reset to the native VLAN ID 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.

Command Default Level

Level: 12.

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 interface eth1/0/1 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)#
```

110-15 vlan

This command is used to add VLANs and enter the VLAN configuration mode. Use the **no** 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.
,	Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is required before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is required before and after the hyphen.

Default

The VLAN ID 1 exists in the system as the default VLAN.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **vlan** global configuration 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)#
```

110-16 vlan precedence

This command is used to specify the VLAN classification precedence for the port. Use **no** command to reset the VLAN classification precedence for the port.

vlan precedence {mac-vlan | subnet-vlan}

no vlan precedence

Parameters

mac-vlan	Specifies the port MAC-based VLAN classification is precedence than the subnet-based VLAN.

subnet-vlan	Specifies the port subnet-based VLAN classification is precedence than MAC-based VLAN.

Default

By default, this option is Mac-based VLAN.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

By default, the precedence to classify the VLAN for an untagged packet is MAC-based > Subnet-based > Protocol VLAN. Use the **vlan precedence** command to configure the VLAN classification precedence between MAC-based VLAN and subnet-based VLAN. The command only takes effect on hybrid or dot1q tunnel interfaces.

Example

This example shows how to configure the interface eth1/0/1 as a subnet VLAN has higher precedence.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# vlan precedence subnet-vlan
Switch(config-if)#
```

110-17 name

This command is used to specify the name of a VLAN. Use the **no** command to reset the VLAN name to the default VLAN name.

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.

Command Default Level

Level: 12.

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)#
```

111. Virtual Private LAN Service (VPLS) Commands

111-1 clear mac-address-table vpls

This command is used to clear the VPLS MAC address.

clear mac-address-table vpls dynamic {all | *VPLS-NAME* **[peer** *IP-ADDRESS* **[***VC-ID***] | ac** *INTERFACE-ID* **[vlan** *VLAN-ID***] | address** *MAC-ADDR***]}**

Parameters

all	Specifies that all dynamic VPLS MAC address will be cleared.
VPLS-NAME	(Optional) Specifies the VPLS name. This name can be up to 32 characters long.
peer	(Optional) Specifies the peer in the VPLS.
IP-ADDRESS	(Optional) Specifies the LSR ID that is used to identify the PE to which the peer belongs to.
VC-ID	(Optional) Specifies the Pseudo-Wire (PW) ID. The range is from 1 to 4294967295.
ac	(Optional) Specifies the local AC in the VPLS.
INTERFACE-ID	(Optional) Specifies the interface ID.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID.
address *MAC-ADDR*	(Optional) Specifies the MAC address to be cleared.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear VPLS MAC addresses.

Example

This example shows how to clear all VPLS MAC addresses.

```
Switch# clear mac-address-table vpls dynamic all
Switch#
```

111-2 l2 vfi manual

This command is used to create a VPLS instance and enter the VFI configuration mode. Use the **no** form of the command to delete a VPLS instance.

l2 vfi *VPLS-NAME* **manual**

no l2 vfi *VPLS-NAME* **manual**

Parameters

VPLS-NAME	Specifies the VPLS instance name. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a VPLS instance and enter the VFI configuration mode. The VPLS name is used to locally identify a unique VPLS on the switch.

Example

This example shows how to create a VPLS instance named “vpls100” and enter the VFI configuration mode.

```
Switch# configure terminal
Switch(config)# l2 vfi vpls100 manual
Switch(config-vfi)#
```

111-3 mtu

This command is used to configure the local AC link MTU value of a VPLS. Use the **no** form of the command to restore the default setting.

mtu *VALUE*

no mtu

Parameters

VALUE	Specifies the local AC link’s MTU value of a VPLS that will be advertised to remote peers in this VPLS. The MTU value must be same at both the local and remote sites to establish the PW. If the MTU is specified as 0, then local the MTU will not be advertised to remote peers in the VPLS. The valid range of value is from 0 to 65535.

Default

By default, this value is 1500.

Command Mode

VFI Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to set the local AC link's MTU value of a VPLS. The local AC link's MTU value can be modified only when there is no PW in this VPLS.

Example

This example shows how to configure the local AC link's MTU value to 1000.

```
Switch# configure terminal
Switch(config)# l2 vfi vpls100 manual
Switch(config-vfi)# mtu 1000
Switch(config-vfi)#
```

111-4 neighbor remote

This command is used to create a peer in a VPLS. Use the **no** command to delete a peer from a VPLS.

neighbor remote *IP-ADDRESS* **[***VC-ID***] encapsulation mpls [no-split-horizon]**

no neighbor remote *IP-ADDRESS* **[***VC-ID***]**

Parameters

IP-ADDRESS	Specifies the LSR ID that is used to identify the PE to which the peer belongs to.
VC-ID	(Optional) Specifies the PW ID. The range is from 1 to 4294967295. It is used with the IP address to uniquely identify a peer for a VPLS. If not specified, the PW ID is set by the VPN ID of this VPLS.
no-split-horizon	(Optional) Specifies that a peer is used as the spoke PW. The packets from other PWs in the VPLS can be forwarded to this PW and the packets from this PW can be forwarded to other PWs in the VPLS. If this option is not specified, the peer is used as a network PW. The packets from other network PWs in a VPLS must not be forwarded to this PW and the packets from this PW must not be forwarded to other network PWs in the VPLS.

Default

By default, the VC ID is set by VPN ID of this VPLS and it is a network PW.

Command Mode

VFI Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a peer in a VPLS. Use the **no** command to delete a peer from a VPLS.

Example

This example shows how to create a peer, which an IP address of 2.2.2.2 and a VC ID of 100. It is a spoke PW.

```
Switch# configure terminal
Switch(config)# l2 vfi vpls100 manual
Switch(config-vfi)# neighbor remote 2.2.2.2 100 encapsulation mpls no-split-horizon
Switch(config-vfi)#
```

111-5 neighbor remote backup

This command is used to create a backup peer for PW redundancy of an H-VPLS.

neighbor remote *IP-ADDRESS* **[***VC-ID***] backup [delay {***DISABLE-DELAY* **| never}]**

Parameters

IP-ADDRESS	Specifies the LSR ID that is used to identify the PE to which the peer belongs to.
VC-ID	(Optional) Specifies the PW ID. The range is from 1 to 4294967295. It is used with the IP address to uniquely identify a peer for a VPLS. If not specified, the PW ID is set by the VPN ID of this VPLS.
DISABLE-DELAY	(Optional) Specifies to switch back to the primary PW with the specified delay time after the primary PW comes online. The range is from 0 to 180 seconds.
never	(Optional) Specifies not switch back to the primary PW even if it comes back online.

Default

By default, the VC ID is set by the VPN ID of this VPLS.

Command Mode

VFI Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a backup peer for PW redundancy of an H-VPLS. For PW redundancy of the H-VPLS, the device will act as an MTU-s and there should be one primary PW and one backup PW configured.

In a normal situation, the primary PW is link-up and the backup PW is link-standby. The packet forwarding between MTU-s and PEs will work in the primary PW. When the LDP hello procedure or other situations find that the primary PW is link-down, the backup PW will be changed to link-up to will take over packet forwarding between MTU-s and PEs.

If the primary PW is recovered, the switch will either keep using the backup PW or switch back to the primary PW base on the delay option setting.

When the backup PW is changed from link-standby to link-up, the MAC withdraw message with a NULL MAC list will be sent from MTU-s to the PE via the backup PW to clear old MAC addresses. When the primary PW is back to link-up and backup PW is changed from link-up to link-standby. A MAC withdraw message with a NULL MAC list will be sent from MTU-s to the PE via the primary PW to clear old MAC addresses.

To delete a backup peer in a VPLS, use **no** command. If the primary PW is deleted in the H-VPLS, the backup peer will become a normal peer.

Example

This example shows how to create a backup peer with an IP address of 2.2.2.2 and the VC ID is set by the VPN ID.

```
Switch# configure terminal
Switch(config)# l2 vfi vpls100 manual
Switch(config-vfi)# neighbor remote 2.2.2.1 encapsulation mpls
Switch(config-vfi)# neighbor remote 2.2.2.2 backup
Switch(config-vfi)#
```

111-6 pw-type

This command is used to set the type of emulated service in a VPLS. Use the **no** form of the command to restore the default setting.

pw-type {raw | tagged}

no pw-type

Parameters

raw	Specifies that the service type is in the Ethernet-raw mode. It means that the encapsulation of all PWs in the VPLS is in the Ethernet-raw mode.
tagged	Specifies that the service type is in the Ethernet-tagged mode. It means that the encapsulation of all PWs in the VPLS is in the Ethernet-tagged mode.

Default

By default, this option is configured as Ethernet-tagged mode.

Command Mode

VFI Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to set the type of emulated service in a VPLS. All PWs of a VPLS should have the same encapsulation as the emulated service type of the VPLS. The service type of a VPLS can be modified only when there is no PW in this VPLS.

Example

This example shows how to set the service type of a VPLS to Ethernet-raw mode.

```
Switch# configure terminal
Switch(config)# l2 vfi vpls100 manual
Switch(config-vfi)# pw-type raw
Switch(config-vfi)#
```

111-7 show mac-address-table vpls

This command is used to display VPLS MAC address information.

show mac-address-table vpls [*VPLS-NAME* **[peer** *IP-ADDRESS* **[***VC-ID***] | ac** *INTERFACE-ID* **[vlan** *VLAN-ID***]]] [address** *MAC-ADDR***]**

Parameters

VPLS-NAME	(Optional) Specifies the VPLS name. This name can be up to 32 characters long.
peer	(Optional) Specifies the peer in a VPLS.
IP-ADDRESS	(Optional) Specifies the LSR ID that is used to identify the PE to which the peer belongs to.
VC-ID	(Optional) Specifies the PW ID. The range is from 1 to 4294967295.
ac	(Optional) Specifies the local AC in a VPLS.
INTERFACE-ID	(Optional) Specifies the Ethernet interface of a local AC.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID.
address *MAC-ADDR*	(Optional) Specifies the MAC address.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display VPLS MAC address information.

Example

This example shows how to display all VPLS MAC address information.

```
Switch# show mac-address-table vpls

VPLS Name                               MAC Address         Peer (VC ID/IP) or AC
------------------------------- ---------------- -------------------------
vpls100                                 00-08-A1-79-9A-DF  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E0  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E1  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E2  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E3  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E4  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E5  101/1.1.1.1
vpls100                                 00-08-A1-79-9A-E6  101/1.1.1.1

Total Entries: 8

Switch#
```

111-8 show mpls l2transport vc

This command is used to display VC information for VPWS and VPLS.

show mpls l2transport vc [*VC-ID*] [detail]

Parameters

VC-ID	(Optional) Specifies the PW ID. The range is from 1 to 4294967295.
detail	(Optional) Specifies to display detailed VC information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display VC (detailed) information for VPWS and VPLS.

Example

This example shows how to display all VC information including VPWS and VPLS.

```
Switch# show mpls l2transport vc

VC ID         Peer              Local AC           MTU        Type     Oper Status
 ---------- -------------- ---------------- -------- ------  -----------
 1             150.1.1.4        eth1/0/0-VLAN2    1500      Raw      Up
 2             130.1.1.2        eth1/0/1-VLAN3    1500      Tagged   Down
 3             140.1.1.2        vpls100             1500      Tagged   Up
 4             160.1.1.2        vpls100             1500      Tagged   Standby
 5             120.1.1.2        vpls101             1500      Tagged   Up

Total Entries: 5

Switch#
```

This example shows how to display detailed VC information for a VPLS.

```
Switch# show mpls l2transport vc 5 detail

VC ID: 5, Peer IP Address: 120.1.1.2, Operate Status: Up
   Local AC: vpls101, Status: Up
Remote AC Status: Up
   MPLS VC Labels: Local 19, Remote 19
   Outbound Tunnel label: 103
   MTU: Local 1500, Remote 1500
   Group ID: Local 0, Remote 0
   Signaling Protocol: LDP
```

```
   Local VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   Remote VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   VC Statistics:
     RX Bytes: 0, RX Packets: 0
     TX Bytes: 0, TX Packets: 0

 Total Entries: 1

Switch#
```

111-9 show vpls

This command is used to display VPLS information.

show vpls [*VPLS-NAME***] [detail]**

Parameters

VPLS-NAME	(Optional) Specifies the VPLS name. This name can be up to 32 characters long.
detail	(Optional) Specifies to display detailed VPLS information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display VPLS (detailed) information.

Example

This example shows how to display all VPLS information.

```
Switch# show vpls

VPLS Name                              VPN ID      Peers/ACs   Oper Status
 ---------------------------------  ----------  ---------  -----------
 vpls100                              100             3/1          Up
 vpls101                              101             3/1          Up
 vpls102                              102             3/1          Up
 vpls103                              103             3/1          Up
 vpls104                              104             3/1          Up
 vpls105                              105             3/1          Up
 vpls106                              106             3/1          Up
```

```
 vpls107                                  107             3/1           Down

Total Entries: 8

Switch#
```

This example shows how to display all VPLS detailed information.

```
Switch# show vpls detail

VPLS Name: vpls100, Operate Status: Up
     VPLS ID: 100, Service Type: Tagged, MTU: 1500
     Peers via Pseudowires:
       VC ID         Peer                Type     Oper Status
       ----------  ---------------  -------  -----------
       100           3.3.3.3            Network  Down
       100           1.1.1.1            Network  Up
       100           5.5.5.5            Spoke     Down
     Local ACs:
       Local AC              Oper Status
       -----------------  -----------
       eth1/0/7-VLAN100       Up

 VPLS Name: vpls101, Operate Status: Up
     VPLS ID: 101, Service Type: Tagged, MTU: 1500
     Peers via Pseudowires:
       VC ID         Peer                Type     Oper Status
       ----------  ---------------  -------  -----------
       101           3.3.3.3            Network  Down
       101           1.1.1.1            Network  Up
       101           5.5.5.5            Spoke     Down
     Local ACs:
       Local AC              Oper Status
       -----------------  -----------
       eth1/0/7-VLAN101       Up

Total Entries: 2

Switch#
```

This example shows how to display VPLS detailed information for a VPLS with PW redundancy.

```
Switch# show vpls vpls102 detail

VPLS Name: vpls102, Operate Status: Up
     VPLS ID: 102, Service Type: Tagged, MTU: 1500
     Peers via Pseudowires:
       VC ID         Peer                Type     Oper Status
       ----------  ---------------  -------  -----------
       100           1.1.1.1            Primary  Up
       100           2.2.2.2            Backup    Standby
     Local ACs:
       Local AC              Oper Status
       -----------------  -----------
```

```
       eth1/0/7-VLAN102       Up

Total Entries: 1

Switch#
```

111-10 vpn id

This command is used to configure the VPN ID of a VPLS.

vpn id *VPN-ID*

Parameters

VPN-ID	Specifies the VPN ID of a VPLS. The value range is from 1 to 4294967295.

Default

None.

Command Mode

VFI Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the VPN ID of a VPLS. Each VPLS in a device should have a local unique VPN ID.

Example

This example shows how to configure the VPN ID of a VPLS to 100.

```
Switch# configure terminal
Switch(config)# l2 vfi vpls100 manual
Switch(config-vfi)# vpn id 100
Switch(config-vfi)#
```

111-11 xconnect vfi

This command is used to create a local AC in a VPLS. Use the **no** command delete a local AC from a VPLS.

xconnect vfi *VPLS-NAME*

no xconnect vfi *VPLS-NAME*

Parameters

VPLS-NAME	(Optional) Specifies the VPLS name. This name can be up to 32

characters long.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a local AC in a VPLS in the interface configuration mode. A local AC could be an Ethernet-based AC which is created in the Ethernet interface or an Ethernet VLAN-based AC which is created in the interface service configuration mode. All local ACs in a VPLS should have same AC type. All VLAN-based local ACs in a VPLS should have the same encapsulation service VLAN.

Example

This example shows how to create a local AC, which is an Ethernet-based AC and the Ethernet port is 1/0/1 into a VPLS which name is “vpls100”.

```
Switch# configure terminal
Switch(config)# interface Ethernet1/0/1
Switch(config-if)# xconnect vfi vpls100
Switch(config-if)#
```

This example shows how to create a local AC, which is an Ethernet VLAN-based AC and the Ethernet port is 2/0/1 and VLAN is 100 into a VPLS which name is “vpls200”.

```
Switch# configure terminal
Switch(config)# interface Ethernet2/0/1
Switch(config-if)# service encapsulation svid 100
Switch(config-if-srv)# xconnect vfi vpls200
Switch(config-if-srv)#
```

112. Virtual Private Wire Service (VPWS) Commands

112-1 backup peer

This command is used to create the PW redundancy of VPWS on the interface. Use the **no** command to cancel the Pseudo-Wire (PW) redundancy of the VPWS service.

backup peer *IP-ADDRESS VC-ID* **[delay {***DISABLE-DELAY* **| never}]**

no backup peer *IP-ADDRESS VC-ID*

Parameters

IP-ADDRESS	Specifies the peer LSR ID that is used to identify the other end Provider Edge (PE).
VC-ID	Specifies the PW service instance ID. It is used to uniquely identify the VPWS and it must be unique at both PEs. The range is from 1 to 4294967295.
DISABLE-DELAY	(Optional) Specifies to switch back to the primary PW with the specified delay time after the primary PW comes back. The range is from 0 to 180 seconds.
never	(Optional) Specifies not to switch back to the primary PW even if it comes back. This is the default option.

Default

None.

Command Mode

Xconnect Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command can be used to enable PW redundancy of a VPWS service. It will create a backup PW. The backup PW will have the same PW type and MTU as the primary PW. There should be one primary PW and one backup PW set up for PW redundancy of the VPWS service. In a normal situation, the primary PW is link up and the backup PW is link standby. The packet forwarding in the VPWS service will take the primary PW. When the LDP hello procedure or other situations found the primary PW to be link down, the backup PW will be changed to link up to do packet forwarding in the VPWS service.

If the primary PW is recovered later, the switch will either keep using the backup PW or switch back to the primary PW base on the delay option setting. The local and remote labels for the backup PW are automatically assigned and exchanged. Generally, when backup PW is setup, the primary PW label is also automatically assigned.

Only one backup PW can be configured.

Example

This example shows how to configure PW redundancy for a VPWS, which will add a backup PW to the remote PE.

```
Switch# configure terminal
```

```
Switch(config)# interface ethernet1/2/1
Switch(config-if)# service encapsulation svid 10
Switch(config-if-srv)# xconnect 130.1.1.2 2 encapsulation mpls
Switch(config-if-xconn)# backup peer 120.1.1.2 3
Switch(config-if-xconn)#
```

This example shows how to configure the switch to back up to the primary PW 10 seconds after the primary PW comes back online.

```
Switch# configure terminal
Switch(config)# interface ethernet1/0/2
Switch(config-if)# service encapsulation svid 10
Switch(config-if-srv)# xconnect 130.1.1.2 2 encapsulation mpls
Switch(config-if-xconn)# backup peer 120.1.1.2 3 delay 10
Switch(config-if-xconn)#
```

112-2 mpls label

This command is used to assign the local label and the remote label used by the manual PW.

mpls label *LOCAL-LABEL REMOTE-LABEL*

no mpls label

Parameters

LOCAL-LABEL	Specifies the incoming label by which the packets of the PW are identified.
REMOTE-LABEL	Specifies the output label used to encapsulate the packet transmitted to the PW.

Default

None.

Command Mode

Xconnect Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available when the manual option is specified in the **xconnect** command. That is, the local label and remote label are manual assigned. If the manual option is not specified, the local and remote labels are assigned and exchanged by the LDP protocol. The service will only be started after the label is assigned.

Example

This example shows how to assign the local label and the remote label for a manual PW.

```
Switch# configure terminal
Switch(config)# interface ethernet1/0/2
Switch(config-if)# service encapsulation svid 10
Switch(config-if-srv)# xconnect 130.1.1.2 2 encapsulation mpls manual
```

```
Switch(config-if-xconn)# mpls label 100 200
Switch(config-if-xconn)#
```

112-3 ping mpls pseudowire

This command is used to check the connectivity of the PW.

ping mpls pseudowire *IP-ADDRESS VC-ID* **[repeat** *COUNT* **| timeout** *SECONDS***]**

Parameters

IP-ADDRESS	Specifies the peer LSR ID that is used to identify the other end PE.
VC-ID	Specifies the PW service instance ID.
repeat *COUNT*	Specifies the number of times to send the same packet. The value range is from 1 to 255 and the default value of times is 4.
timeout *SECONDS*	Specifies the interval in seconds to send the MPLS request packet. The value range is from 1 to 99 seconds and the default value is 2 seconds.

Default

None.

Command Mode

EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to check the connectivity of the PW. If there is no LSP for the specified PW, the “Destination unreachable” message will be displayed. Otherwise, VCCV messages will be sent out to along the LSP of the specified PW. For static PWs, the VCCV message will use the CC type 2 and CV type LSP ping. For PWs using LDP as the signaling method, the CC type and CV type is negotiated by LDP. If the peer received the request message, it will reply the request message sender with MPLS echo reply message. If the sender cannot receive reply before timeout, the “Request timed out” message will be displayed.

Example

This example shows how to check the connectivity of the PW with peer address 192.1.1.0 and VC ID 1.

```
Switch# ping mpls pseudowire 192.1.1.0 1

Reply from 192.1.1.0, time<10ms
Reply from 192.1.1.0, time<10ms
Reply from 192.1.1.0, time<10ms
Reply from 192.1.1.0, time<10ms

Ping Statistics for FEC: VC 1/192.1.1.0
Packets: Sent =4, Received =4, Lost =0

Switch#
```

This example shows how to check the connectivity of the PW with peer address 110.1.1.0 and VC ID 2.

```
Switch# ping mpls pseudowire 110.1.1.0 2

Request timed out.
Request timed out.
Request timed out.
Request timed out.

Ping Statistics for FEC: VC 2/110.1.1.0
Packets: Sent =4, Received =0, Lost =4

Switch#
```

112-4 service encapsulation svid

This command is used to create a service instance on a switch port and enter the interface service configuration mode with a specified encapsulation service VLAN ID.

service encapsulation svid *VLAN-ID*

Parameters

VLAN-ID	Specifies the encapsulation VLAN number.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Issuing this command will create or enter the interface service configuration mode with a specified encapsulation service VLAN ID. The user can further configure the VPLS or VPWS AC using the **xconnect** command. If the interface service configuration is exit without issuing the **xconnect** command, the service is automatically deleted.

Example

This example shows how to create an interface service and enter the interface service configuration mode with service VLAN 1000 on switch port eth2/0/1 and setup an AC to VPWS VC 2.

```
Switch# configure terminal
Switch(config)# interface ethernet2/0/1
Switch(config-if)# service encapsulation svid 1000
switch(config-if-srv)# xconnect 110.1.1.12 2 encapsulation mpls
Switch(config-if-xconn)#
```

112-5 show mpls l2transport vc

This command is used to display the VPWS VC information.

show mpls l2transport vc [*VC-ID*] [detail]

Parameters

VC-ID	Specifies the display the specified PW ID only.
detail	Specifies the display detailed PW information.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to display the VPWS VC information.

Example

This example shows how to display information of all VCs.

```
Switch# show mpls l2transport vc

VC ID         Peer              Local AC        MTU        Type     Oper Status
 ------------ ------------- ---------------- ---------- ---------  -----------
 1             150.1.1.4        eth1/0/1-VLAN2      1500    Raw      Up
 2             130.1.1.2        eth1/0/1-VLAN3      1500    Tagged  Down
 3             140.1.1.2        eth1/0/1-VLAN4      1500    Tagged  Up
 4             160.1.1.2        eth1/0/1-VLAN4      1500    Tagged  Standby

Total Entries: 4

Switch#
```

This example shows how to display detailed information of VC 1.

```
Switch# show mpls l2transport vc 1 detail

VC ID: 1, Peer IP Address: 150.1.1.4, Operate Status: Up
  Local AC: eth1/0/1-VLAN2, Status: Up
Remote AC Status: Up
   MPLS VC Labels: Local 16, Remote 16
   Outbound Tunnel label: 100
   MTU: Local 1500, Remote 1500
   Group ID: Local 0, Remote 0
   Signaling Protocol: LDP
   Local VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   Remote VCCV Capabilities:
```

```
      CC: Type 2
      CV: LSP ping
VC Statistics:
     RX Bytes: 0, RX Packets: 0
     TX Bytes: 0, TX Packets: 0

 Total Entries: 1

Switch#
```

This example shows how to display detailed information belonging to PW redundancy.

```
Switch# show mpls l2transport vc detail

VC ID: 3, Peer IP Address: 140.1.1.2, Operate Status: Up, Primary
  Local AC: eth1/0/1-VLAN4, Status: Up
Remote AC Status: Up
   MPLS VC Labels: Local 17, Remote 17
   Outbound Tunnel label: 101
   MTU: Local 1500, Remote 1500
   Group ID: Local 0, Remote 0
   Signaling Protocol: LDP
   Local VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   Remote VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   VC Statistics:
     RX Bytes: 0, RX Packets: 0
     TX Bytes: 0, TX Packets: 0

VC ID: 4, Peer IP Address: 160.1.1.2, Operate Status: Standby, Backup
  Backup Delay: Never
  Local AC: eth1/0/1-VLAN4, Status: Up
Remote AC Status: Up
   MPLS VC Labels: Local 18, Remote 18
   Outbound Tunnel label: 102
   MTU: Local 1500, Remote 1500
   Group ID: Local 0, Remote 0
   Signaling Protocol: LDP
   Local VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   Remote VCCV Capabilities:
      CC: Type 2
      CV: LSP ping
   VC Statistics:
     RX Bytes: 0, RX Packets: 0
     TX Bytes: 0, TX Packets: 0

 Total Entries: 2

Switch#
```

112-6 xconnect

This command is used to create the VPWS service on the interface. Use the **no** form of this command to remove the VPWS service.

xconnect *IP-ADDRESS VC-ID* **encapsulation mpls [manual] [raw | tagged] [mtu 0-65535]**

no xconnect

Parameters

IP-ADDRESS	Specifies the peer LSR ID that is used to identify the other end PE.
VC-ID	Specifies the PW service instance ID. The range is from 1 to 4294967295.
raw	(Optional) Specifies that the PW type is in the Ethernet-raw mode. For this type, S-tags will not be sent over the PW.
tagged	(Optional) Specifies that the PW type is in the Ethernet-tag mode. For this type, S-tags will be sent over the PW. By default, the PW type is in the Ethernet-tag mode.
mtu	(Optional) Specifies the local CE-PE link MTU that will be advertised to remote peer. If specifies the MTU to 0, the LDP will not advertise the local MTU. The MTU must be same at both local and remote. Otherwise, the PW will not be setup. The valid range of this value is from 0 to 65535. If not specified, the default MTU value is 1500.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create a VPWS service and enter the Xconnect configuration mode. When creating the VPWS on a physical port or link aggregation group, the service is Ethernet-based and this Ethernet port or link aggregation group is the AC. When creating the VPWS on a VLAN sub-interface of a switch port interface, the service is Ethernet VLAN-based and this VLAN sub-interface of the switch port is the AC.

Use the **no xconnect** command to remove a VPWS service. The settings related to the service are also removed.

Example

This example shows how to configure the AC from the Customer Edge Bridge (CE) to the PE as the VLAN 10 of port 1. Assume the VC's ID is 2. For making the VLAN 10 packets from CE one can be transmitted to the other end through the MPLS network. Configure PE1 and PE2 as follows.

Configuring PE 1:

```
Switch# configure terminal
Switch(config)# interface ethernet1/0/1
Switch(config-if)# service encapsulation svid 10
```

```
Switch(config-if-srv)# xconnect 130.1.1.2 2 encapsulation mpls
Switch(config-if-xconn)#
```

Configuring PE 2:

```
Switch# configure terminal
Switch(config)# interface ethernet1/0/1
Switch(config-if)# service encapsulation svid 10
Switch(config-if-srv)# xconnect 110.1.1.12 2 encapsulation mpls
Switch(config-if-xconn)#
```

113. Virtual Router Redundancy Protocol (VRRP) Commands

113-1 vrrp ip

This command is used to create a VRRP group on an interface. Use the **no** form of this command to remove a VRRP group.

vrrp *VRID* **ip** *IP-ADDRESS*

no vrrp VRID

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.
IP-ADDRESS	Specifies the IP address for the created virtual router group.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command creates a virtual router and specifies the IP address for the virtual router. All routers in the same VRRP group must be configured with the same virtual router ID and IP address.

A virtual router group is represented by a virtual router ID. The IP address of the virtual router is the default router configured on hosts. The virtual router's IP address can be a real address configured on the routers, or an unused IP address. If the virtual router address is a real IP address, the router that has this IP address is the IP address owner.

A master will be elected in a group of routers that supports the same virtual routers. Others are the backup routers. The master is responsible for forwarding the packets that are sent to the virtual router.

Example

This example shows how to create a VRRP group on interface VLAN 1. The virtual router identifier is 7, and 10.1.1.1 is the IP address of the virtual router.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# vrrp 7 ip 10.1.1.1
Switch(config-if)#
```

113-2 vrrp non-owner-ping

This command is used to enable the virtual router in the master state to respond to ICMP echo requests for an IP address not owned but associated with this virtual router. Use the **no** form of this command to

disable the virtual router in the master state to respond to ICMP echo requests for an IP address not owned but associated with this virtual router.

vrrp non-owner-ping

no vrrp non-owner-ping

Parameters

None.

Default

By default, the virtual router in the master state does not response the ICMP echo requests for an IP address that is not owned by this virtual router.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In some conditions, the virtual router in the master state needs to response ICMP echo requests for an IP address that is not owned by this virtual router.

Example

This example shows how to enable all virtual routers to respond to ICMP echo requests.

```
Switch# configure terminal
Switch(config)# vrrp non-owner-ping
Switch(config)#
```

113-3 vrrp timers advertise

This command is used to configure the interval between successive VRRP advertisements by the master router. To restore the default value, use the **no** form of this command.

vrrp *VRID* **timers advertise** *INTERVAL*

no vrrp *VRID* **timers advertise**

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.
INTERVAL	Specifies the time interval between successive advertisements by the master router. The unit of the interval is in seconds. The valid value is from 1 to 255.

Default

By default, this value is 1 second.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The maser will constantly send VRRP advertisements to communicate the related information of the current master virtual router. This command configures the interval between advertisement packets and the time before other routers declare the master router as down. All routers in a VRRP group must use the same timer values.

Example

This example shows how to configure the router to send advertisements for VRRP 7 every 10 seconds on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# vrrp 7 timers advertise 10
Switch(config-if)#
```

113-4 vrrp priority

This command is used to configure the priority of a virtual router. To restore the default priority, use the **no** form of this command.

vrrp *VRID* **priority** *PRIORITY*

no vrrp *VRID* **priority**

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.
PRIORITY	Specifies the priority of the virtual router. A higher value means a higher priority. The valid range is from 1 to 254.

Default

By default, this value is 100.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The master of a virtual router is elected based on the priority setting. The router that owns the virtual router IP address has the highest priority to be elected.

The router with the highest priority will become the master, and other routers with a lower priority will then act as the backup for the virtual router. Each router should be configured with different priority values. If there are multiple routers with the same highest priority value, the router with the highest numbers in its IP address will become the master.

The router that is the IP address owner of the VRRP group is always the master of the VRRP group.

Example

This example shows how to configure the priority of VRRP group 7 to be 200 on interface VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# vrrp 7 priority 200
Switch(config-if)#
```

113-5 vrrp preempt

This command is used to allow a router to take over the master role if it has a better priority than the current master. Use the **no** form of the command to change back to non-preempt mode.

vrrp *VRID* **preempt**

no vrrp *VRID* **preempt**

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In preempt mode, a router will take over the master role if it has a better priority than the current master.

In non-preempt mode, the master will not be preempted unless the incoming router is the IP address owner of the virtual router.

Example

This example shows how to configure the router for VRRP group 7 to preempt the current master router when its priority of 200 is higher than that of the current master router.

```
Switch# configure terminal
Switch(config)# interface vlan1
Switch(config-if)# vrrp 7 preempt
Switch(config-if)#
```

113-6 vrrp track critical-ip

This command is used to configure the critical IP address of a virtual router. Use the **no** form of this command to remove the critical IP address.

vrrp *VRID* **track critical-ip** *IP-ADDRESS*

no vrrp *VRID* **track critical-ip**

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.
IP-ADDRESS	Specifies the critical IP address.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to set the critical IP address for one virtual router. If the critical IP is configured on one virtual router, the virtual router cannot be activated when the critical IP address is unreachable. One VRRP group can only track one critical IP.

Example

This example shows how to configure the critical IP address of virtual router 1 on VLAN 1.

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp 1 track critical-ip 192.168.100.1
Switch(config-if)#
```

113-7 vrrp authentication

This command is used to enable VRRP authentication and set the password on an interface. Use the **no** form of this command to remove the authentication.

vrrp authentication *STRING*

no vrrp authentication

Parameters

STRING	Specifies the plain text authentication password (8 bytes).

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable VRRP authentication on an interface. The authentication is applied to all virtual routers on this interface. The devices in the same VRRP group must have the same authentication password.

Example

This example shows how to configure one interface's VRRP authentication:

```
Switch# configure terminal
Switch(config)# interface vlan 1
Switch(config-if)# vrrp authentication test
Switch(config-if)#
```

113-8 show vrrp

This command is used to display the VRRP status.

show vrrp [interface *INTERFACE-ID* **[***VRID***]]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID.
VRID	(Optional) Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the VRRP related setting and status.

Example

This example shows how to display the VRRP status for all interfaces.

```
Switch# show vrrp

vlan1 – VRID 7
  State is Master
  Virtual IP address is 20.1.1.1
  Virtual MAC address is 00-00-5e-00-01-07
  Advertisement interval is 1 seconds
  Preemption is enabled
  Priority is 255
  No critical IP address
  Master router is 20.0.1.1 (local)

vlan1 – VRID 8
  State is Master
```

```
  Virtual IP address is 20.1.1.2
  Virtual MAC address is 00-00-5e-00-01-08
  Advertisement interval is 1 seconds
  Preemption is disabled
  Priority is 200
  Critical IP address is 20.2.3.4
  Master router is 20.0.1.2 (local)

vlan2 – VRID 5
  State is Initialize
  Virtual IP address is 30.1.1.254
  Virtual MAC address is 00-00-5e-00-01-05
  Advertisement interval is 1 seconds
  Preemption is enabled
  Priority is 100
  No critical IP address
  Master router is unknown

vlan3 – VRID 1
  State is Backup
  Virtual IP address is 50.1.1.254
  Virtual MAC address is 00-00-5e-00-01-01
  Advertisement interval is 1 seconds
  Preemption is disabled
  Priority is 80
  No critical IP address
  Master router is 50.0.1.2

Total Entries: 4

Switch#
```

113-9 show vrrp brief

This command is used to display the VRRP brief status.

show vrrp brief

Parameters

None.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display VRRP brief status.

Example

This example shows how to display the brief VRRP information.

```
Switch#show vrrp brief

Interface VRID Pri    Owner Pre State   Master IP      VRouter IP
--------- ---- ----  ------ --- ------ -------------- -------------
vlan1     7    255       Y   Y  Master  20.0.1.1       20.0.1.1
vlan1     8    200           Y  Master  20.0.1.1       20.1.1.2
vlan2     5    100           Y  Init    0.0.0.0        30.1.1.254
vlan3     1    80            Y  Backup  50.0.1.2       50.1.1.254

Total Entries: 4

Switch#
```

Display Parameters

Interface	The Interface ID.
VRID	The virtual router identifier.
Pri	The VRRP priority value.
Owner	“Y” Indicates that the virtual router is the IP address owner.
Pre	Indicates if preempt mode is enabled or not. “Y” indicates preempt mode is enabled.
State	The state of the virtual router.
Master IP	The IP address of the master virtual router.
VRouter IP	The IP address of the virtual router.

113-10 debug vrrp

This command is used to turn on the VRRP debug function. Use the **no** form of the command to turn off VRRP debug function.

debug vrrp

no debug vrrp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn on or turn off the VRRP debug function.

Example

This example shows how to turn on the VRRP debug function.

```
Switch# debug vrrp
Switch#
```

113-11 debug vrrp errors

This command is used to on the VRRP error prompt debug switch. Use the **no** form of the command to turn off VRRP error prompt debug switch.

debug vrrp errors

no debug vrrp errors

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn on or turn off the VRRP error prompt debug switch.

Example

This example shows how to turn on the VRRP error prompt debug switch.

```
Switch# debug vrrp errors
Switch#

Received an ADV msg with incorrect checksum on VR 1 at interface System
Received an ADV msg with incorrect checksum on VR 1 at interface System
Received an ADV msg with incorrect checksum on VR 1 at interface System
```

113-12 debug vrrp events

This command is used to turn on the VRRP event debug switch. Use the **no** form of the command to turn off VRRP event debug switch.

debug vrrp events

no debug vrrp events

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn on or turn off the VRRP event debug switch.

Example

This example shows how to turn on the VRRP event debug switch.

```
Switch# debug vrrp events
Switch#

interface ip100 link up
interface ip100 link down
Master received a higher priority ADV msg at VR 2 at interface System
Master received a higher priority ADV msg at VR 2 at interface System
Authentication type mismatch on VR 1 at interface System
```

113-13 debug vrrp packets

This command is used to turn on the VRRP packet debug switch. Use the **no** form of the command to turn off VRRP packet debug switch.

debug vrrp packets

no debug vrrp packets

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn on or turn off the VRRP packet debug switch.

Example

This example shows how to turn on the VRRP packet debug switch.

```
Switch# debug vrrp packets
Switch#

Received an ADV msg at VR 2 on interface System
Received an ADV msg at VR 2 on interface System
Received an ADV msg at VR 2 on interface System
Send out an ADV msg at VR 1 at interface System priority 255
Send out an ADV msg at VR 1 at interface System priority 255
Send out an ADV msg at VR 1 at interface System priority 255
```

113-14 debug vrrp state

This command is used to turn on the VRRP state debug switch. Use the **no** form of the command to turn off VRRP state debug switch.

debug vrrp state

no debug vrrp state

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn on or turn off the VRRP state debug switch.

Example

This example shows how to turn on the VRRP state debug switch.

```
Switch# debug vrrp state
Switch#

VR 1 at interface System switch to Master
VR 2 at interface System switch to Master
VR 1 at interface ip100 switch to Init
```

113-15 debug vrrp log

This command is used to turn on the log of VRRP. Use the **no** form of the command to turn off log of VRRP.

debug vrrp log

no debug vrrp log

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn on or turn off the log of VRRP. When log of VRRP is turned on and there are some VRRP change events, some logs will be recorded.

Example

This example shows how to turn on the log of VRRP.

```
Switch# debug vrrp log
Switch#
```

114. Virtual Routing and Forwarding Lite (VRF-lite) Commands

114-1 address-family ipv4 vrf

This command is used to enter the VRF address family configuration mode. Use the **no** form of this command to remove the VRF address family configuration.

address-family ipv4 vrf *VRF-NAME*

no address-family ipv4 vrf *VRF-NAME*

Parameters

VRF-NAME	Specifies the name of the VRF.

Default

None.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used for configuring the routing instances such as BGP or RIP (IPv4) that use IPv4 address prefixes. After executing this command, the address family configuration mode will be entered and a new routing instance may be created with this command. For example, in RIP, with this command, a new RIP routing instance will be created. If the **no** form of this command is executed, the related routing instance will be removed.

Example

This example shows how to create a new RIP routing instance of VRF VPN-A.

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# exit
Switch(config)# router rip
Switch(config-router)# address-family ipv4 vrf VPN-A
Switch(config-router-af)#
```

114-2 import map

This command is used to configure the import route map of one VRF. Use the **no** form of this command to delete the import route map.

import map *ROUTE-MAP*

no import map

Parameters

ROUTE-MAP	Specifies the name of import route map of the VRF.

Default

None.

Command Mode

VRF Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the import route map of one VRF. This is used by the routing protocol to filter the routes imported to the routing table associated with a VRF instance. One VRF only has one import route map. The new import route map will overwrite the value set before.

Example

This example shows how to create a VRF VPN-A and set its import route map.

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# import map rmap1
Switch(config-vrf)#
```

114-3 ip vrf

This command is used to create a new VRF instance. Use the **no** form of this command to delete one VRF instance.

ip vrf *VRF-NAME*

no ip vrf *VRF-NAME*

Parameters

VRF-NAME	Specifies the name of the VRF.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create a new VRF instance and enter the VRF Configuration Mode. After a new VRF instance is created, a new VRF routing table will be created. With the **no** form of this command, one VRF will be deleted. The related VRF routing table will be deleted at the same time and all routing instances based on this VRF will be destroyed. All IP interfaces associated to this VRF will be restored to the global routing instance. In the other words, all configurations based on this VRF will be removed.

Example

This example shows how to create and delete a VRF instance.

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# exit
Switch(config)# no ip vrf VPN-A
Switch(config)#
```

114-4 ip vrf forwarding

This command is used to associate one interface to a VRF instance. Use the **no** form of this command to restore one interface to the global routing instance.

ip vrf forwarding *VRF-NAME*

no ip vrf forwarding

Parameters

VRF-NAME	Specifies the name of the VRF.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to associate an interface to one VRF instance. By associating interfaces to different VRFs, the interfaces in different VRFs can be configured with the same IP address. The IP address space in one VRF is individual and can overlap among different VRFs.

Example

This example shows how to associate the VLAN 100 interface to the VRF VPN-A.

```
Switch# configure terminal
Switch(config)# int vlan 100
Switch(config-if)# ip forwarding vrf VPN-A
Switch(config-if)# ip address 100.1.1.1 255.255.255.0
Switch(config-if)#
```

114-5 maximum routes

This command is used to limit the maximum routes within the VRF. Use the **no** form of this command to remove the limit.

maximum routes *LIMIT* **{***WARN-THRESHOLD* **| warning-only}**

no maximum routes

Parameters

LIMIT	Specifies the maximum number of routes within the VRF. Its range is from 1 to 16384.
WARN-THRESHOLD	Specifies the warning threshold value in percentage. A notification message will be sent when the routes number reach the threshold and no more routes can be written into the hardware. Its range is from 1 to 100.
warning-only	Specifies that when the route numbers exceeds the threshold, a notification message will be sent, but more routes can be written into hardware.

Default

By default, there is no limit.

Command Mode

VRF Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to limit how many routes can be allowed within the VRF. This limit only applies to the active route. To only get a notification, set the warning-only option.

Example

This example shows how to configure the VRF VPN-A's routes limit to 100.

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# maximum routes 100 warning-only
Switch(config-vrf)#
```

114-6 rd

This command is used to configure the Route Distinguisher (RD) of one VRF.

rd *ROUTE-DISTINGUISHER*

Parameters

ROUTE-DISTINGUISHER	Specifies the VRF's route distinguisher, which is used to prepend an 8-bytes value to an IPv4 prefix to create a VPN-IPv4 prefix.

Default

None.

Command Mode

VRF Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the VRF's route distinguisher to form a unique VPN-IPv4 prefix. One VRF has only one route distinguisher and cannot be changed if it has been set to one value.

Specify an RD in one of the following two forms:

- **ASN-related** - It is formed by an AS number and an arbitrary number. For example, 123:2.
- **IP-address-related** - It is formed by an IP address and an arbitrary number. For example, 10.2.3.4:3.

Example

This example shows how to create an VRF instance VPN-A and set its route distinguisher.

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# rd 100:1
Switch(config-vrf)#
```

114-7 route-target

This command is used to add one route target of a VRF. Use the **no** form of this command to remove one route target.

route-target {import | export | both} *ROUTE-TARGET*

no route-target {import | export | both} *ROUTE-TARGET*

Parameters

import	Specifies to add an import route target to the import routing information from the target VPN extended community.
export	Specifies to add an export route target to the export routing information to the target VPN extended community.
both	Specifies to add both the import route target and export route target.
ROUTE-TARGET	Specifies the value of the route target.

Default

None.

Command Mode

VRF Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to add a route target to one VRF. The route target is a useful VPN application. One VRF can have multiple route targets.

Example

This example shows how to create a VRF instance VPN-A and add import and export targets.

```
Switch# configure terminal
Switch(config)# ip vrf VPN-A
Switch(config-vrf)# route-target import 100:1
Switch(config-vrf)# route-target export 100:1
Switch(config-vrf)#
```

114-8 show ip vrf

This command is used to display VRF settings.

show ip vrf [details | interfaces] [*VRF-NAME***]**

Parameters

details	(Optional) Specifies to display detailed information about one or more VRFs.
interfaces	(Optional) Specifies to display interfaces associated with one or more VRFs.
VRF-NAME	(Optional) Specifies to display information associated with one VRF.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to check the settings of VRF instances.

Example

This example shows how to check the current VRF's settings.

```
Switch# show ip vrf

VRF Name              RD                   Interfaces
----------------- ------ -------------------- ---------------------
VPN-A                 100:1                ip100
VPN-B                 Not set

Switch#
```

This example shows how to check detailed information about VRF VPN-A.

```
Switch# show ip vrf details VPN-A

VRF VPN-A; default RD: 100:1
  Interfaces:
```

```
    ip100
  Export VPN route-target communities:
    RT:100:1
  Import VPN route-target communities:
    RT:100:1
  Import route-map: rmap1
  Route Warning Limit 5, Current Count 0

Switch#
```

This example shows how to check interfaces associated with VRFs.

```
Switch# show ip vrf interfaces

Interfaces   IP Address         VRF
------------ ------------------ ------------
ip100        100.1.1.1/24       VPN-A

Switch#
```

115. Web Authentication Commands

115-1 web-auth enable

This command is used to enable the Web authentication function on the port. Use the **no** form of this command to disable the Web authentication function.

web-auth enable

no web-auth enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command allows hosts connected to the port to do authentication via the Web browser.

Example

This example shows how to enable the Web authentication function on interface eth1/0/1.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# web-auth enable
Switch(config-if)#
```

115-2 web-auth page-element

This command is used to customize the Web authentication page elements. Use the **no** form of this command to return to the default setting.

web-auth page-element {page-title *STRING* **| login-window-title** *STRING* **| username-title** *STRING* **| password-title** *STRING* **| logout-window-title** *STRING* **| copyright-line** *LINE-NUMBER* **title** *STRING***}**

no web-auth page-element {page-title | login-window-title | username-title | password-title | logout-window-title | copyright-line}

Parameters

page-title *STRING*	Specifies the title of the Web authentication page. The maximum number can be up to 128 characters.
login-window-title *STRING*	Specifies the title of the Web authentication login window. The

	maximum number can be up to 64 characters.
username-title *STRING*	Specifies the user name title of Web authentication login window. The maximum number can be up to 32 characters.
password-title *STRING*	Specifies the password title of Web authentication login window. The maximum number can be up to 32 characters.
logout-window-title *STRING*	Specifies the title of the Web authentication logout window. The maximum number can be up to 64 characters.
copyright-line *LINE-NUMBER* **title** *STRING*	Specifies the copyright information by lines in Web authentication pages. The total copyright information can be up to 5 lines and 128 characters for each line.

Default

By default, the page title is not set.

By default, the login window title is “Authentication Login”.

By default, the username title is “User Name”.

By default, the password title is “Password”.

By default, the logout window title is “Logout From The Network”.

By default, the copyright information is not set.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Administrators can customize Web authentication page elements. There are two Web authentication pages, (1) the authentication login page and (2) the authentication logout page.

The Web authentication login page will be displayed to the user to get the username and password when the system doing Web authentication for the user.

Users can logout from the network by clicking the **Logout** button on the authentication login page after success login to the network.

Example

This example shows how to modify two lines of the copyright information at the bottom of the authentication page with:

Line 1: Copyright @ 2013 All Rights Reserved

Line 2: Site: http://support.website.com

```
Switch# configure terminal
Switch(config)# web-auth page-element copyright-line 1 title Copyright @ 2013 All
Rights Reserved
Switch(config)# web-auth page-element copyright-line 2 title Site:
http://support.website.com
Switch(config)#
```

115-3 web-auth success redirect-path

This command is used to configure the default URL the client Web browser will be redirected to after successful authentication. Use the **no** form of this command to remove the specification.

web-auth success redirect-path *STRING*

no web-auth success redirect-path

Parameters

STRING	Specifies the default URL the client Web browser will be redirected to after successful authentication. If no default redirect URL is specified, the Web authentication logout page will be displayed. The default redirect path can be up to 128 characters.

Default

By default, the Web authentication logout page is displayed.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the Web page to display to the hosts who passes the Web authentication.

Example

This example shows how to configure the default redirect path to be “http://www.website.com” after passing Web authentication.

```
Switch# configure terminal
Switch(config)# web-auth success redirect-path http://www.website.com
Switch(config)#
```

115-4 web-auth system-auth-control

This command is used to enable the Web authentication function globally on the switch. Use the **no** form of this command to disable the Web authentication function globally on the switch.

web-auth system-auth-control

no web-auth system-auth-control

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Web authentication is a feature designed to authenticate a user by using the Web browser when the user is trying to access the Internet via the switch. The switch itself can be the authentication server and do the authentication based on a local database or be a RADIUS client and perform the authentication process via RADIUS protocol with remote RADIUS server. The authentication process uses either the HTTP or HTTPS protocol.

Example

This example shows how to enable the Web authentication function globally on the switch.

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

115-5 web-auth virtual-ip

This command is used to configure the Web authentication virtual IP address which is used to accept authentication requests from host. Use the **no** form of this command to return to the default setting.

web-auth virtual-ip {ipv4 *IP-ADDRESS* **| ipv6** *IPV6-ADDRESS* **| url** *STRING***}**

no web-auth virtual-ip {ipv4 | ipv6 | url}

Parameters

ipv4 *IP-ADDRESS*	Specifies the Web authentication virtual IPv4 address.
url *STRING*	Specifies the FQDN URL for Web authentication The FQDN URL can be up to 128 characters.
ipv6 *IPV6-ADDRESS*	Specifies the Web authentication virtual IPv6 address.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The virtual IP of Web authentication is just the characterization of the Web authentication function on the switch. All Web authentication processes communicate with this IP address, however, the virtual IP does not respond to any ICMP packet or ARP request. So it's not allowed to configure virtual IP in the same subnet as the switch's IP interface or the same subnet as the host PCs' subnet, otherwise the Web authentication cannot operate correctly.

The defined URL only takes effect when the virtual IP address is configured. The users get the FQDN URL stored on the DNS server to get the virtual IP address. The obtained IP address must match the virtual IP address configured by the command.

If the IPv4 virtual IP is not configured, the IPv4 access cannot start a Web authentication. If the IPv6 virtual IP is not configured, the IPv6 access cannot start a Web authentication.

Example

This example shows how to configure the Web authentication virtual IPv4 to be “1.1.1.1” and the FQDN URL to be “www.website4.co”.

```
Switch# configure terminal
Switch(config)# web-auth virtual-ip  ipv4 1.1.1.1
Switch(config)# web-auth virtual-ip  url www.website4.co
Switch(config)#
```

This example shows how to Switch# configure terminal configure the Web authentication virtual IPv6 to be “2000::2” and the FQDN URL to be “www.website6.co”.

```
Switch# configure terminal
Switch(config)# web-auth virtual-ip ipv6 2000::2
Switch(config)# web-auth virtual-ip url www.website6.co
Switch(config)#
```

116. Weighted Random Early Detection (WRED) Commands

116-1 clear random-detect drop-counter

This command is used to clear WRED drop counters.

clear random-detect drop-counter {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	(Optional) Specifies to clear all counters.
interface *INTERFACE-ID* **[,	-]**	(Optional) Specifies the interface ID to be cleared. Specify multiple interface IDs, which are separated by commas (,) or hyphens (-). No space is before or after the commas or hyphens.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Only physical ports are valid for this command.

Example

This example shows how to clear WRED drop counters on eth 3/0/1.

```
Switch# clear random-detect drop-counter interface eth3/0/1
Switch#
```

116-2 random-detect

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

random-detect *COS-VALUE* **[profile** *ID***]**

no random-detect *COS-VALUE*

Parameters

COS-VALUE	Specifies the CoS queues on which the WRED state will be set. The valid range is from 0 to 7.
profile *ID*	(Optional) Specifies the WRED profile that will be applied. If not

	specified, the default threshold setting is used.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When a packet arrives, the current average queue size is calculated by hardware.

$$avg\_Qsize = current\_Qsize + \frac{old\_avg\_Qsize - current\_Qsize}{2^{weight}}$$

If the current average queue size is less than the minimum threshold value of the queue, the arriving packet is queued. If the current queue length is between the minimum threshold value and the maximum threshold value of the queue, the packet is either dropped or queued depending on the packet drop probability. The drop probability is calculated by the following formula.

$$Drop\,\mathrm{Pr}\,obability = \frac{avg\_Qsize - MinThreshold}{MaxThreshold - MinThreshold} * MaxDropRate$$

If the average queue size is greater than the maximum threshold value of the queue, all packets will be dropped. If the specified profile does not exist, then default setting of the threshold will be associated.

Example

This example shows how to enable the WRED function on eth3/0/1 queue 5 and apply the WRED profile 10.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# random-detect 5 profile 10
Switch(config-if)#
```

116-3 random-detect ecn

This command is used to enable the explicit congestion notification (ECN).Use the **no** form of the command to disable it.

random-detect ecn *COS-VALUE*

no random-detect ecn *COS-VALUE*

Parameters

COS-VALUE	Specifies the CoS queues on which ECN will be enabled or disabled. The valid range is from 0 to 7.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

WRED drops packets, based on the average queue size exceeding a specific threshold, to indicate congestion. ECN is an extension to WRED in that ECN marks packets instead of dropping them when the average queue size exceeds a specific threshold value. When configuring the WRED Explicit Congestion Notification feature, routers and end hosts would use this marking as a signal that the network is congested and slow down sending packets.

As stated in RFC 3168 (ECN to IP), the ECN field has two bits. The ECN-capable transport (ECT) bit and the Congestion Experienced (CE) bit in the IP header. Each of the ECT and CE bits combination list as follows:

ECT Bit	CE Bit	Indicates
0	0	Not ECN capable,
0	1	ECN capable
1	0	ECN capable
1	1	Congestion experienced

The following points explain how packets are treated when ECN is enabled:

- If the ECT and CE bit is (0,0), the packets are dropped based on the WRED drop probability.
- If the ECT and CE bit is (0,1) or (1,0), the WRED determines that the packet should be dropped based on the drop probability, then the ECT and CE bits for the packet are changed to 1 instead of dropping them, and the packet is transmitted.
- If the ECT and CE bit is (1,1), the packet is transmitted. No further marking is required

Example

This example shows how to enable ECN on eth 3/0/1 queue 5.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# random-detect ecn 5
Switch(config-if)#
```

116-4 random-detect exponential-weight

This command is used to configure the WRED exponential weight factor for the average queue size calculation for the queue. Use the **no** form of the command to reset to the default setting.

random-detect exponential-weight *COS-VALUE* **exponent** *VALUE*

no random-detect exponential-weight *COS-VALUE*

Parameters

COS-VALUE	Specifies CoS queues on which the exponent will be set. The valid range is from 0 to 7.
exponent *VALUE*	Specifies the exponent value from 0 to 15.

Default

The default exponential weight factor is 9.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the WRED exponential weight factor for the average queue size calculation for the queue.

Example

This example shows how to configure the exponent value to 10 on eth3/0/1 queue 5.

```
Switch# configure terminal
Switch(config)# interface eth3/0/1
Switch(config-if)# random-detect exponential-weight 5 exponent 10
Switch(config-if)#
```

116-5 random-detect profile

This command is used to configure the WRED profile. Use the **no** form of this command to reset to the default setting.

random-detect profile *ID* **[tcp | non-tcp] [green | yellow | red] min-threshold** *VALUE* **max-threshold** *VALUE* **max-drop-rate** *VALUE*

no random-detect profile *ID*

Parameters

profile *ID*	Specifies the ID of the WRED profile that will be set.
tcp	Specifies the WRED drop parameters for the TCP packets to be set.
non-tcp	Specifies the WRED drop parameters for non-TCP packets to be set.
green	Specifies the WRED drop parameters for green packets to be set.
yellow	Specifies the WRED drop parameters for yellow packets to be set.
red	Specifies the WRED drop parameters for red packets to be set.
min-threshold *VALUE*	Specifies the minimum queue size (in cells) to start WRED dropping.
max-threshold *VALUE*	Specifies the maximum queue size (in cells) over which WRED will drop all packets destined for this queue.
max-drop-rate *VALUE*	Specifies the drop probability when the average queue size reaches the maximum threshold. When this value is zero, then the packet will not be dropped or remarked for ECN.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Different types of packets can be queued in different bucket lists and different list can be specified with different threshold values.

Example

This example shows how to configure the WRED drop parameter for all types and color packets on profile 10.

```
Switch# configure terminal
Switch(config)# random-detect profile 10 min-threshold 30 max-threshold 50 max-drop rate 10
Switch(config)#
```

This example shows how to configure the WRED drop parameter for TCP yellow and red packets on profile 10.

```
Switch# configure terminal
Switch(config)# random-detect profile 10 tcp yellow red min-threshold 20 max-threshold 40 max-drop rate 5
Switch(config)#
```

116-6 show queueing random-detect

This command is used to display the WRED configuration on the specified interface.

show queueing random-detect [interface *INTERFACE-ID* **[,|-]]**

Parameters

interface *INTERFACE-ID* **[, | -]**	(Optional) Specifies the interface ID to be displayed. Specify multiple interface IDs, which are separated by commas (,) or hyphens (-). No space is before or after the commas or hyphens.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

This command will display the WRED configuration. If interface ID is not specified, the WRED configuration for all ports on the system will be displayed.

Example

This example shows how to display the WRED configuration and CoS queue status on eth 1/0/1.

```
Switch# show queueing random-detect interface eth1/0/1
```

```
Current WRED configuration:
  eth1/0/1
  CoS   WRED State      Exp-weight-constant   Profile
  ---   ----------      -------------------   -------
    0   Enabled          9                         1
    1   Enabled          9                         1
    2   Enabled          9                         1
    3   Enabled          9                         1
    4   Enabled          9                         1
    5   Enabled          9                         1
    6   Enabled          9                         1
    7   Enabled          9                         1

Switch#
```

116-7 show random-detect drop-counter

This command is used to display the WRED drop counter.

show random-detect drop-counter [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	Specifies the interface ID for which the WRED drop counter will be displayed. You can specify multiple interface IDs, which are separated by commas (,) or hyphens (-). No space is before or after the commas or hyphens.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the WRED drop counter.

Example

This example shows how to display the WRED drop counter on eth 1/0/1.

```
Switch# show random-detect drop-counter interface eth1/0/1

Current WRED Drop Counter:

Interface    Green      Yellow      Red
----------  --------   --------   --------
Eth1/0/1     0            5           10

Switch#
```

116-8 show random-detect profile

This command is used to display the WRED profile setting.

show random-detect profile [profile *ID***]**

Parameters

profile *ID*	(Optional) Specifies the WRED profile ID that will be displayed. If not specified, the configuration for all WRED profiles will be displayed.

Default

None.

Command Mode

User EXEC or Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the WRED profile setting.

Example

This example shows how to display the WRED profile 1 settings.

```
Switch# show random-detect profile 1

WRED Profile 1
Packet Type      Min-Threshold   Max-Threshold   Max-Drop-Rate
-----------      -------------   -------------   -------------
TCP-Green        50                 80                1
TCP-Yellow       40                 60                5
TCP-Red          30                 50                8
Non-TCP-Green    20                 40                10
Non-TCP-Yellow   15                 30                10
Non-TCP-Red      10                 20                10

Switch#
```

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DXS-3600 Series switch.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords will be forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the **Password Recovery** feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on this switch to easily recover passwords.

Complete these steps to reset the password:

- For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
- Power on the Switch. After the **UART init** is loaded to 100%, the switch will allow 2 seconds for the user to press the hotkey [**^**] (**Shift+6**) to enter the “Password Recovery Mode.” Once the Switch enters the “Password Recovery Mode,” all ports on the Switch will be disabled.

```
  Boot Procedure                                          V1.10.008
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address    : 00-17-9A-14-6B-10
  H/W Version    : B1

  Please Wait, Loading V2.00.012 Runtime Image ..............  100 %
  UART init .................................................  100 %
```

```
Password Recovery Mode

Switch(reset-config)#
```

In the “Password Recovery Mode” only the following commands can be used.

no enable password	This command is used to delete all account level passwords.
no login password	This command is used to clear the local login methods.
no username	This command is used to delete all local user accounts.
password-recovery	This command is used to initiate the password recovery procedure.
reload	This command is used to save and reboot the switch.
reload clear running-config	This command is used to reset the running configuration to the factory default settings and then reboot the switch.
show running-config	This command is used to display the current running configuration.
show username	This command is used to display local user account information.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this switch.

802.1X

Log Description	Severity
Event description: 802.1X Authentication failure. 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. username: The user that is being authenticated.. interface-id: The interface name. macaddr: The MAC address of thr authenticated device.	Warning
Event description: 802.1X authentication success (Username: <username>, <interface-id>, MAC: <mac-address>) Parameters description: username: The user that is being authenticated. interface-id: The interface name. macaddr: The MAC address of the authenticated device.	Informational

AAA

Log Description	Severity
Event description: This log will be generated when AAA global state is enabled or disabled. Log Message: AAA is <status>. Parameters description: status: The status indicates the AAA enabled or disabled.	Informational
Event description: This log will be generated when login successfully. Log Message: Successful login through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. Username: It indicates the username for authentication.	Informational
Event description: This log will be generated when login failure. Log Message: Login failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description:	Warning

exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	
Event description: This log will be generated when the remote server does not respond to the login authentication request. Log Message: Login failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address. username: It indicates the username for authentication.	Warning
Event description: This log will be generated when enable privilege successfully. Log Message: Successful enable privilege through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: none, local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. Username: It indicates the username for authentication.	Informational
Event description: This log will be generated when enable privilege failure. Log Message: Enable privilege failed through <exec-type> <from client-ip> authenticated by AAA <aaa-method> <server-ip> (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. aaa-method: It indicates the authentication method, e.g.: local, server. server-ip: It indicates the AAA server IP address if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event description: This log will be generated when the remote server does not respond to the enable password authentication request. Log Message: Enable privilege failed through <exec-type> <from client-ip> due to AAA server <server-ip> timeout (Username: <username>). Parameters description: exec-type: It indicates the EXEC types, e.g.: Console, Telnet, SSH, Web, Web(SSL). client-ip: It indicates the client's IP address if valid through IP protocol. server-ip: It indicates the AAA server IP address. username: It indicates the username for authentication.	Warning

Event description: This log will be generated when RADIUS assigned a valid VLAN ID attributes. Log Message: RADIUS server <server-ip> assigned VID: <vid> to port <interface-id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. vid: The assign VLAN ID that authorized by from RADIUS server. interface–id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
Event description: This log will be generated when RADIUS assigned a valid bandwidth attributes. Log Message: RADIUS server <server-ip> assigned <direction> bandwidth: <threshold> to port < interface -id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. Direction: It indicates the direction for bandwidth control, e.g.: ingress or egress. Threshold: The assign threshold of bandwidth that authorized by from RADIUS server. interface–id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
Event description: This log will be generated when RADIUS assigned a valid priority attributes. Log Message: RADIUS server <server-ip> assigned 802.1p default priortiy: <priority> to port < interface -id> (Username: <username>) Parameters description: server-ip: It indicates the RADIUS server IP address. priority: The assign priority that authorized by from RADIUS server. interface–id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
Event description: This log will be generated when RADIUS assigned ACL script but fails to apply to the system due to insufficient resource. Log Message: RADIUS server <server-ip> assigns <username> ACL failure at port < interface -id> (<acl-script>) Parameters description: server-ip: It indicates the RADIUS server IP address. username: It indicates the username for authentication. interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server.	Warning

BGP

Log Description	Severity
Event description: BGP FSM with Peer has gone to the successfully established state. Log Message: BGP-6-ESTABLISH: BGP connection is successfully established (Peer:<ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Informational

Event description: BGP connection is normally closed. Log Message: BGP-6-NORMALCLOSE: BGP connection is normally closed (Peer:<ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Informational
Event description: BGP connection is closed due to error (Error Code, Error Subcode and Data fields Refer to RFC). Log Message: BGP-4-ERRCLOSE: BGP connection is closed due to error (Code:<num> Subcode:<num> Field:<field> Peer:<ipaddr>). Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. field: field value when an error happen. ipaddr: IP address of the BGP peer.	Warning
Event description: Receive a BGP notify packet with an undefined error code or sub error code in RFC 4271. Log Message: BGP-4-RCVUNKOWNERR: BGP Notify: unkown Error code(num), Sub Error code(num), Peer:<ipaddr>. Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.	Warning
Event description: Receive a BGP update packet but the next_hop points to a local interface. Log Message: BGP-4-BADNHOP: BGP Update Attr NHop: Erroneous NHop <ipaddr> Peer:<ipaddr>. Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP connection is closed due to some events happens. (Event refer to RFC) Log Message: BGP-4-EVENTCLOSE: BGP connection is closed due to Event: <num> (Peer:<ipaddr>). Parameters description: num: Event is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.	Warning
Event description: BGP connection is closed due to receive notify packet. (Error Code and Error Subcode refer to RFC) Log Message: BGP-4-NOTIFYCLOSE: BGP connection is closed due to Notify: Code <num> Subcode <num> (Peer:<ipaddr>). Parameters description: num: Error Code or Error Subcode is defined in RFC 4271 etc. ipaddr: IP address of BGP peer.	Warning
Event description: The number of bgp prefix received from this neighbor reaches the threshold. Log Message: BGP-6-PEERPFXMAX: The number of prefix received reaches <num>, max <limit> (Peer < ipaddr >). Parameters description: num: The number of prefix received. limit: Max number of prefix allowed to receive. ipaddr: IP address of BGP peer.	Information
Event description: The total bgp prefix number received exceeds the limit.	Information

Log Message: BGP-6-TOTALPFXMAX: The total number of prefix received reaches max prefix limit.	
Event description: BGP received unnecessary AS4-PATH attribute from new (4-bytes AS) BGP peer Log Message: BGP-4-RCVUNNECEAS4PATH: Received AS4-PATH attribute from new (4-bytes AS) peer. (Peer <ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP received unnecessary AS4-AGGREGATOR attribute from new (4-bytes AS) BGP peer Log Message: BGP-4-RCVUNNECEAS4AGGRE: Received AS4-AGGREGATOR attribute from new (4-bytes AS) peer. (Peer <ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. Log Message: BGP-4-RCVASCONFEDINAS4PATH: Received AS_CONFED_SEQUENCE or AS_CONFED_SET path segment type in AS4-PATH attribute. (Peer <ipaddr>). Parameters description: ipaddr: IP address of BGP peer.	Warning
Event description: BGP received invalid AS4-PATH attribute. Log Message: BGP-4-RCVBADAS4PATH: Received invalid AS4-PATH attribute. Value : <STRING> (Peer <ipaddr>). Parameters description: STRING: Detailed description about the invalid attribute. ipaddr: IP address of BGP peer.	Warning
Event description: BGP received invalid AS4- AGGREGATOR attribute. Log Message: BGP-4-RCVBADAS4AGGRE: Received invalid AS4-AGGREGATOR attribute. Value : <STRING> (Peer <ipaddr>). Parameters description: STRING: Detailed description about the invalid attribute. ipaddr: IP address of BGP peer.	Warning

BPDU Protection

Log Description	Severity
Event description: Record the event when the BPDU attack happened. Log Message: <interface-id> enter STP BPDU under protection state (mode: <mode>) Parameters description: interface-id: Interface on which detected STP BPDU attack. mode: BPDU Protection mode of the interface. Mode can be drop, block, or shutdown	Informational
Event description: Record the event when the STP BPDU attack recovered. Log Message: <interface-id> recover from BPDU under protection state. Parameters description: interface-id: Interface on which detected STP BPDU attack.	Informational

CFM

Log Description	Severity
Event description: Cross-connect is detected Log Message: CFM cross-connect. VLAN:<vlanid>, Local(MD Level:<mdlevel>, Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros mean unknown MAC address. Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.	Critical
Event description: Error CFM CCM packet is detected Log Message: CFM error ccm. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Remote(MEPID:<mepid>, MAC:<macaddr>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Can be "inward" or "outward". mepid: Represents the MEPID of the MEP. The value 0 means unknown MEPID. macaddr: Represents the MAC address of the MEP. The value all zeros means unknown MAC address. Note: In CFM hardware mode, remote MEP information (mepid and macaddr) is unknown.	Warning
Event description: cannot receive the remote MEP's CCM packet Log Message: CFM remote down. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Warning
Event description: Remote MEP's MAC reports an error status Log Message: CFM remote MAC error. MD Level:<mdlevel>, VLAN:<vlanid>,	Warning

Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	
Event description: Remote MEP detects CFM defects Log Message: CFM remote detects a defect. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the MEP direction, which can be "inward" or "outward". mepid: Represents the MEPID of the MEP. macaddr: Represents the MAC address of the MEP.	Informational

CFM Extension

Log Description	Severity
Event description: AIS condition detected Log Message: AIS condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice
Event description: AIS condition cleared Log Message: AIS condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice

Event description: LCK condition detected Log Message: LCK condition detected. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice
Event description: LCK condition cleared Log Message: LCK condition cleared. MD Level:<mdlevel>, VLAN:<vlanid>, Local(Port <[unitID:]portNum>, Direction:<mepdirection>, MEPID:<mepid>) Parameters description: vlanid: Represents the VLAN identifier of the MEP. mdlevel: Represents the MD level of the MEP. unitID: Represents the ID of the device in the stacking system. portNum: Represents the logical port number of the MEP. mepdirection: Represents the direction of the MEP. This can be "inward" or "outward". mepid: Represents the MEPID of the MEP.	Notice

Configuration/Firmware

Log Description	Severity
Event description: Firmware upgraded successfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational
Event description: Firmware upgraded unsuccessfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning
Event description: Firmware uploaded successfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description:	Informational

unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	
Event description: Firmware uploaded unsuccessfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning
Event description: Configuration downloaded successfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational
Event description: Configuration downloaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Warning
Event description: Configuration uploaded successfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr : Represent client MAC address.	Informational
Event description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters description: unitID: The unit ID. session: The user's session. username: Represent current login user.	Warning

	ipaddr: Represent client IP address. macaddr : Represent client MAC address.

DDM

Log Description	Severity
Event description: DDM exceeded or recover from DDM alarm threshold Log Message: Optical transceiver <interface-id> [component] [high-low] alarm threshold [exceedType] Parameters description: interface-id: The port number. component: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. high-low: High or low threshold. exceedType: indicate exceed threshold or recover to normal event, the value should be “exceeded” or “exceeding back to normal”	Critical
Event description: DDM exceeded or recover from DDM warning threshold Log Message: Optical transceiver <interface-id> [component] [high-low] warning threshold [exceedType] Parameters description: interface-id: The port number. component: the DDM threshold type. The value should be one of the following values: temperature, supply voltage, bias current, TX power, RX power. high-low: High or low threshold. exceedType: indicate exceed threshold or recover to normal event, the value should be “exceeded” or “exceeding back to normal”	Warning

DHCPv6 Client

Log Description	Severity
Event description: DHCPv6 client interface administrator state changed. Log Message: DHCPv6 client on interface <ipif-name> changed state to [enabled | disabled]. Parameters description: <ipif-name>: Name of the DHCPv6 client interface.	Informational
Event description: 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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: The ipv6 address obtained from a DHCPv6 server starts renewing. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> starts renewing. Parameters description:	Informational

ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	
Event description: 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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: 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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: 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: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface..	Informational
Event description: The ipv6 address from a DHCPv6 server was deleted. Log Message: The IPv6 address < ipv6address > on interface <ipif-name> was deleted. Parameters description: ipv6address: ipv6 address obtained from a DHCPv6 server. ipif-name: Name of the DHCPv6 client interface.	Informational
Event description: DHCPv6 client PD interface administrator state changed. Log Message: DHCPv6 client PD on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: DHCPv6 client PD obtains an IPv6 prefix from a delegation router. Log Message: DHCPv6 client PD obtains an ipv6 prefix < ipv6networkaddr> on interface <intf-name> Parameters description: ipv6networkaddr: ipv6 preifx obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router starts renewing. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts renewing. Parameters description: ipv6networkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router renews	Informational

success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> renews success. Parameters description: ipv6anetworkaddr: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD nterface.	
Event description: The IPv6 prefix obtained from a delegation router starts rebinding. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> starts rebinding. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix obtained from a delegation router rebinds success. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> rebinds success. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational
Event description: The IPv6 prefix from a delegation router was deleted. Log Message: The IPv6 prefix < ipv6networkaddr > on interface <intf-name> was deleted. Parameters description: ipv6address: IPv6 prefix obtained from a delegation router. intf-name: Name of the DHCPv6 client PD interface.	Informational

DHCPv6 Relay

Log Description	Severity
Event description: DHCPv6 relay on a specify interface's administrator state changed Log Message: DHCPv6 relay on interface <ipif-name> changed state to [enabled | disabled] Parameters description: <ipif-name>: Name of the DHCPv6 relay agent interface.	Informational

DHCPv6 Server

Log Description	Severity
Event description: The address of the DHCPv6 Server pool is used up Log Message: The address of the DHCPv6 Server pool <pool-name> is used up. Parameters description: <pool-name>: Name of the DHCPv6 Server pool.	Informational
Event description: The number of allocated ipv6 addresses is equal to 4096 Log Message: The number of allocated ipv6 addresses of the DHCPv6 Server pool is equal to 4096.	Informational

Parameters description:

DLMS

Log Description	Severity
Event Description: Input an illegal activation code. Log Message: Illegal activation code (AC: <string25>). Parameters Description: <string25>: Activation Code	Informational
Event Description: License Expired. Log Message: License expired (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Critical
Event Description: License successfully installed. Log Message: License successfully installed (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Informational
Event Description:When a license is going to expire, it will be logged before 30 days. Log Message: License will expire in 30 days. (license:<license-model>, AC: <string25>). Parameters Description: <license-model>: License Model Name. <string25>: Activation Code	Informational

DOS Prevention

Log Description	Severity
Event description: Record the event if any attacking packet is received in the interval. Log Message: <dos-type> is dropped from (IP :< ip-address> Port: <interface-id>). Parameters description: dos-type: The type of DoS attack will be one of the followings. ip-address: IP address of attacker. interface-id: the attacked interface.	Notice

DULD

Log Description	Severity
Event description: A unidirectional link has been detected on this port Log Message: <interface-id> is unidirectional. Parameters description: unitID: the unit ID	Informational

portNum: port number	

Dynamic ARP Inspection

Log Description	Severity
Event description: This log will be generated when DAI detect invalid ARP packet. 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 that ARP packet is request or ARP response.	Warning
Event description: This log will be generated when DAI detect valid ARP packet. 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 that ARP packet is request or ARP response.	Informational

ERPS

Log Description	Severity
Event description: Signal failure detected Log Message: Signal failure detected on node <macaddr> Parameters description: macaddr: The system MAC address of the node	Notice
Event description: Signal failure cleared Log Message: Signal failure cleared on node <macaddr> Parameters description: macaddr: The system MAC address of the node.	Notice
Event description: RPL owner conflict Log Message: RPL owner conflicted on the ring <macaddr> Parameters description: macaddr: The system MAC address of the node	Warning

Interface

Log Description	Severity
Event description: Port link up. Log Message: Port < interface-id > link up, <link state> Parameters description: portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex	Informational
Event description: Port link down. Log Message: Port < interface-id > link down Parameters description:	Informational

portNum: 1.Interger value;2.Represent the logic port number of the device.	

IP Directed-Broadcast

Log Description	Severity
Event description: IP Directed-broadcast rate exceed 50 packets per second on a certain subnet. Log Message: IP Directed Broadcast packet rate is high on subnet. [(IP: %s)] Parameters description: IP: the Broadcast IP destination address.	Informational
Event description: IP Directed-broadcast rate exceed 100 packets per second Log Message: IP Directed Broadcast rate is high. Parameters description:	Informational

LACP

Log Description	Severity
Event description: Link Aggregation Group link up. Log Message: Link Aggregation Group < group_id > link up. Parameters description: group_id: The group id of the link down aggregation group.	Informational
Event description: Link Aggregation Group link down. Log Message: Link Aggregation Group < group_id > link down. Parameters description: group_id: The group id of the link down aggregation group.	Informational
Event description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id>. Parameters description: ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
Event description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id>. Parameters description: ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

LBD

Log Description	Severity
Event description: Record the event when an interface detect loop. Log Message: <interface-id> LBD loop occurred. <interface-id > VLAN <vlan-id> LBD loop occurred. Parameters description: interface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	Critical

Event description: Record the event when an interface loop recovered. Log Message: <interface-id> LBD loop recovered. <interface-id> VLAN <vlan-id> LBD loop recovered. Parameters description: nterface-id: Interface on which loop is detected. vlan-id: VLAN on which loop is detected.	Critical
Event description: Record the event when the number of VLANs that loop back has occurred exceeds a reserved number. Log Message: Loop VLAN numbers overflow. Parameters description:	Critical

LLDP-MED

Log Description	Severity
Event description: LLDP-MED topology change 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: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice
Event description: Conflict LLDP-MED device type 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: portNum: The port number. chassisType: chassis ID subtype.	Notice

Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	
Event description: Incompatible LLDP-MED TLV set 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: chassis ID subtype. Value list: 1. chassisComponent(1) 2. interfaceAlias(2) 3. portComponent(3) 4. macAddress(4) 5. networkAddress(5) 6. interfaceName(6) 7. local(7) chassisID: chassis ID. portType: port ID subtype. Value list: 1. interfaceAlias(1) 2. portComponent(2) 3. macAddress(3) 4. networkAddress(4) 5. interfaceName(5) 6. agentCircuitId(6) 7. local(7) portID: port ID. deviceClass: LLDP-MED device type.	Notice

Login/Logout CLI

Log Description	Severity
Event description: Login through console successfully. Log Message: [Unit <unitID>,]Successful login through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through console unsuccessfully. Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Warning
Event description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Login through telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

Event description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Critical
Event description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

MAC

Log Description	Severity
Event description: the host has passed MAC authentication Log Message: MAC-based Access Control host login success (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host has aged out. Log Message: MAC-based Access Control host aged out (MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Informational
Event description: the host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (MAC <macaddress>, <interface-id>, VID: <vlan-id>). Parameters description: mac-address: the host MAC addresses. interface-id: the interface on which the host is authenticated. vlan-id: the VLAN ID on which the host exists.	Critical

Event description: the authorized user number on the whole device has reached the maximum user limit. Log Message: MAC-based Access Control enters stop learning state..	Warning
Event description: the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: MAC-based Access Control recovers from stop learning state.	Warning
Event description: the authorized user number on an interface has reached the maximum user limit. Log Message: <interface-id> enters MAC-based Access Control stop learning state Parameters description: interface-id: the interface on which the host is authenticated.	Warning
Event description: the authorized user number on an interface is below the maximum user limit in a time interval. Log Message: <interface-id> recovers from MAC-based Access Control stop learning state. Parameters description: interface-id: the interface on which the host is authenticated.	Warning

Module

Log Description	Severity
Event Description: Module inserts and can works. Log Message: Module <module-type> is inserted. Parameters Description: module-type: the expansion module name.	Informational
Event Description: Module inserts and can't works. Log Message: Module < module-type > inserts but can't work except reboot device. Parameters Description: module-type: the expansion module name.	Warning
Event Description: Module hot removes. Log Message: Module < module-type > is removed. Parameters Description: module-type: the expansion module name.	Informational

MPLS

Log Description	Severity
Event description: LSP is up Log Message: LSP <lsp_id> is up Parameters description: lsp_id: The established LSP ID	Informational
Event description: LSP is down Log Message: LSP <lsp_id> is down Parameters description: lsp_id: The deleted LSP ID	Informational

MSTP Debug Enhancement

Log Description	Severity
Event description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] , <interface-id> ,MAC: <macaddr>)] Parameters description: InstanceID: Instance ID. portNum:Port ID macaddr: MAC address	Notice
Event description: Spanning Tree new Root Bridge Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected([Instance: <InstanceID>]MAC: <macaddr> Priority :<value>) Parameters description: InstanceID: Instance ID. macaddr: Mac address value: priority value	Informational
Event description: Spanning Tree Protocol is enabled Log Message: Spanning Tree Protocol is enabled	Informational
Event description: Spanning Tree Protocol is disabled Log Message: Spanning Tree Protocol is disabled	Informational
Event description: New root port Log Message: New root port selected [([Instance:<InstanceID>], <interface-id>)] Parameters description: InstanceID: Instance ID. portNum:Port ID	Notice
Event description: Spanning Tree port status changed Log Message: Spanning Tree port status change [([Instance:<InstanceID>], <interface-id>)] <old_status> -> <new_status> Parameters description: InstanceID: Instance ID. portNum: Port ID old_status: Old status new_status: New status	Notice
Event description: Spanning Tree port role changed. Log Message: Spanning Tree port role change. [([Instance:<InstanceID>], <interface-id>)] <old_role> -> <new_role> Parameters description: InstanceID: Instance ID. portNum:Port ID/ old_role: Old role new_status:New role	Informational
Event description: Spannnig Tree instance created. Log Message: Spanning Tree instance create. Instance:<InstanceID> Parameters description: InstanceID: Instance ID.	Informational
Event description: Spannnig Tree instance deleted.	Informational

Log Message: Spanning Tree instance delete. Instance:<InstanceID> Parameters description: InstanceID: Instance ID.	
Event description: Spanning Tree Version changed. Log Message: Spanning Tree version change. New version:<new_version> Parameters description: new_version: New STP version.	Informational
Event description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> ,revision level <revision_level>). Parameters description: name : New name. revision_level:New revision level.	Informational
Event description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational
Event description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table changed (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]). Parameters description: InstanceID: Instance ID. startvlanid- endvlanid:VLANlist	Informational

OSPFv2 Enhancement

Log Description	Severity
Event description: OSPF interface link state changed. Log Message: OSPF-6-INTFSTATECHANGE: OSPF interface <intf-name> changed state to [Up | Down] Parameters description: intf-name: Name of OSPF interface.	Informational
Event description: OSPF interface administrator state changed. Log Message: OSPF-6-INTFADMINCHANGE: OSPF protocol on interface <intf-name> changed state to [Enabled | Disabled Parameters description: intf-name: Name of OSPF interface.	Informational
Event description: One OSPF interface changed from one area to another. Log Message: OSPF-6-INTFAREACHANGE: OSPF interface <intf-name> changed from area <area-id> to area <area-id> Parameters description: intf-name: Name of OSPF interface. area-id: OSPF area ID.	Informational

Event description: One OSPF neighbor state changed from Loading to Full. Log Message: OSPF-5-NBRLOADINGTOFULL: OSPF nbr <nbr-id> on interface <intf-name> changed state from Loading to Full Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
Event description: One OSPF neighbor state changed from Full to Down. Log Message: OSPF-5-NBRFULLTODOWN: OSPF nbr <nbr-id> on interface <intf-name> changed state from Full to Down Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
Event description: One OSPF neighbor state's dead timer expired. Log Message: OSPF-5-DTIMEXPIRED: OSPF nbr <nbr-id> on interface <intf-name> dead timer expired Parameters description: intf-name: Name of OSPF interface. nbr-id: Neighbor's router ID.	Notice
Event description: One OSPF virtual neighbor state changed from Loading to Full. Log Message: OSPF-5-VNBRLOADINGTOFULL: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full Parameters description: nbr-id: Neighbor's router ID.	Notice
Event description: One OSPF virtual neighbor state changed from Full to Down. Log Message: OSPF-5-VNBRFULLTODOWN: OSPF nbr <nbr-id> on virtual link changed state from Full to Down Parameters description: nbr-id: Neighbor's router ID.	Notice
Event description: OSPF router ID was changed. Log Message: OSPF-6-RIDCHANGE: OSPF router ID changed to <router-id> Parameters description: router-id: OSPF router ID.	Informational
Event description: Enable OSPF. Log Message: OSPF-6-STATECHANGE: OSPF state changed to [Enabled | Disabled]	Informational

Peripheral

Log Description	Severity
Event description: Fan Recovered. Log Message: Unit <id>, <fan-descr> back to normal. Parameters description: Unit <id>: The unit ID. fan-descr: The FAN ID and position.	Critical
Event description: Fan Fail Log Message: Unit <id> <fan-descr> failed Parameters description:	Critical

Unit <id>: The unit ID. fan-descr: The FAN ID and position.	
Event description: Temperature sensor enters alarm state. Log Message: Unit <unit-id> <thermal-sensor-descr> detects abnormal temperature <degree> Parameters description: unitID: The unit ID. thermal-sensor-descr: The sensor ID and position. degree: The current temperature.	Critical
Event description: Temperature recovers to normal. Log Message: Unit <unit-id> <thermal-sensor-descr> temperature back to normal Parameters description: unitID: The unit ID. thermal-sensor-descr: The sensor ID and position.	Critical
Event description: Power failed. Log Message: Unit <unit-id> <power-descr> failed Parameters description: unitID: The unit ID. power-descr: The power position and ID.	Critical
Event description: Power is recovered. Log Message: Unit <unit-id> <power-descr> back to normal Parameters description: unitID: The unit ID. power-descr: The power position and ID.	Critical
Event description: Air flow abnormal. Log Message: Unit <unit-id> detecting abnormal air flow. Parameters description: unitID: The unit ID.	Critical
Event description: Air flow recovered. Log Message: Unit <unit-id> abnormal air flow back to normal. Parameters description: unitID: The unit ID.	Critical

Port Security

Log Description	Severity
Event description: Address full on a port 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
Event description: Address full on system Log Message: Limit on system entry number has been exceeded.	Warning

RIPng

Log Description	Severity
Event description: The RIPng state of interface changed Log Message: RIPng-6-INTFSTATECHANGE :RIPng protocol on interface <intf-name> changed state to <enabled | disabled> Parameters description: intf-name: Interface name.	Informational

Safeguard

Log Description	Severity
Event description: When the CPU utilization is over the rising threshold, the switch enters exhausted mode. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode. Parameters description: unit-id: the unit ID	Warning
Event description: When the CPU utilization is lower than the falling threshold, the switch enters normal mode. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode. Parameters description: unit_id: the unit ID.	Informational

SNMP

Log Description	Severity
Event Description: SNMP request received with 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
Event description: SSH server is enabled. Log Message: SSH server is enabled	Informational
Event description: SSH server is disabled. Log Message: SSH server is disabled	Informational
Event description: This log will be generated when SSH log failed (not via AAA method). Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr | ipv6address>). Parameters description: username: User name which logs in fail. ipaddr: IP address of host from which the user logged in.	Critical

ipv6address: IPv6 address of host from which the user logged in.

Stacking

Log Description	Severity
Event description: Hot insertion. Log Message: Unit: <unitID>, MAC: <macaddr> Hot insertion. Parameters description: unitID: Box ID. macaddr: MAC address.	Informational
Event description: Hot removal. Log Message: Unit: <unitID>, MAC: <macaddr> Hot removal. Parameters description: unitID: Box ID. macaddr: MAC address.	Informational
Event description: Stacking topology change. Log Message: Stacking topology is <Stack_TP_TYPE>. Master(Unit <unitID>, MAC:<macaddr>). Parameters description: Stack_TP_TYPE: The stacking topology type is one of the following: 1. Ring, 2. Chain. unitID: Box ID. macaddr: MAC address.	Informational
Event description: Backup master changed to master. Log Message: Backup master changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Slave changed to master Log Message: Slave changed to master. Master (Unit: <unitID>). Parameters description: unitID: Box ID.	Informational
Event description: Box ID conflict. Log Message: Hot insert failed, box ID conflict: Unit <unitID> conflict (MAC: <macaddr> and MAC: <macaddr>). Parameters description: unitID: Box ID. macaddr: The MAC addresses of the conflicting boxes.	Critical

Traffic Control

Log Description	Severity
Event description: Broadcast storm occurrence. Log Message: <interface-id> Broadcast storm is occurring. Parameters description: interface-id: The interface name.	Warning

Event description: Broadcast storm cleared. Log Message: <interface-id> Broadcast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Multicast storm occurrence. Log Message: <interface-id> Multicast storm is occurring. Parameters description: interface-id: The interface name.	Warning
Event description: Multicast Storm cleared. Log Message: <interface-id>Multicast storm has cleared. Parameters description: interface-id: The interface name.	Informational
Event description: Storm us occured. Log Message: <Broadcast | Multicast | Unicast> storm is occurring on <interface-id>. Parameters description: Broadcast: Storm is resulted by broadcast packets(DA = FF:FF:FF:FF:FF:FF). Multicast: Storm is resulted by multicast packets, including unknown L2 multicast, known L2 multicast, unknown IP multicast and known IP multicast. Unicast: Storm is resulted by unicast packets, including both known and unknown unicast packets interface-id: The interface ID on which a storm is occurring.	Warning
Event description: Storm is cleared. Log Message: <Broadcast | Multicast | Unicast> storm is cleared on <interface-id>. Parameters description: Broadcast: Broadcast storm is cleared. Multicast: Multicast storm is cleared. Unicast: Unicast storm (including both known and unknown unicast packets) is cleared. interface-id: The interface ID on which a storm is cleared.	Informational
Event description: Port shut down due to a packet storm Log Message: <interface-id> is currently shut down due to the <Broadcast | Multicast | Unicast> storm. Parameters description: interface-id: The interface name. Broadcast: The interface is disabled by broadcast storm. Multicast: The interface is disabled by multicast storm. Unicast: The interface is disabled by unicast storm (including both known and unknown unicast packets).	Warning

VPLS

Log Description	Severity
Event description: VPLS link up Log Message: VPLS <vpls_name> link up	Informational

Parameters description: vpls_name: The name of the link up VPLS	
Event description: VPLS link down Log Message: VPLS <vpls_name> link down Parameters description: vpls_name: The name of the link down VPLS	Informational

VPWS

Log Description	Severity
Event description: Pseudo-wire link down Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> link down Parameters description: vc_id: The link down Pseudo-wire ID ipaddr: The peer IP address of the link down Pseudo-wire	Informational
Event description: Pseudo-wire link up Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> link up Parameters description: vc_id: The link up Pseudo-wire ID ipaddr: The peer IP address of the link up Pseudo-wire	Informational
Event description: Pseudo-wire is deleted Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> is deleted Parameters description: vc_id: The deleted Pseudo-wire ID ipaddr: The peer IP address of the deleted Pseudo-wire	Informational
Event description: Pseudo-wire link standby Log Message: Pseudo-wire id <vc_id> peer ip <ipaddr> link standby Parameters description: vc_id: The link standby Pseudo-wire ID ipaddr: The peer IP address of the link standby Pseudo-wire	Informational

VRRP Debug Enhancement

Log Description	Severity
Event description: One virtual router state becomes Master. Log Message: VRRP-6-STATEMASTER:VR <vr-id> at interface <intf-name> switch to Master Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
Event description: One virtual router state becomes Backup. Log Message: VRRP-6-STATEBACKUP: VR <vr-id> at interface <intf-name> switch to Backup Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational

Event description: One virtual router state becomes Init. Log Message: VRRP-6-STATEINIT: VR <vr-id> at interface <intf-name> switch to Init Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Informational
Event description: Authentication type mismatch of one received VRRP advertisement message. Log Message: VRRP-4-AUTHTYPEMIS:Authentication type mismatch on VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
Event description: Authentication checking fail of one received VRRP advertisement message. Log Message: VRRP-4-AUTHFAIL: Authentication fail on VR <vr-id> at interface <intf-name>. Auth type <auth-type> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based. Auth-type: VRRP interface authentication type.	Warning
Event description: Checksum error of one received VRRP advertisement message. Log Message: VRRP-4-BADCHK:Received an ADV msg with incorrect checksum on VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
Event description: Virtual router ID mismatch of one received VRRP advertisement message. Log Message: VRRP-4-VRIDMIS: Received ADV msg virtual router ID mismatch. VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
Event description: Advertisement interval mismatch of one received VRRP advertisement message. Log Message: VRRP-4-ADVMIS: Received ADV msg adv interval mismatch. VR <vr-id> at interface <intf-name> Parameters description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	Warning
Event description: A virtual MAC address is added into switch L2 table Log Message: VRRP-5-MACADD: Added a virtual MAC <vrrp-mac-addr> into L2 table Parameters description: vrrp-mac-addr: VRRP virtual MAC address	Notice
Event description: A virtual MAC address is deleted from switch L2 table. Log Message: VRRP-5-MACDEL: Deleted a virtual MAC <vrrp-mac-addr> from L2 table	Notice

Parameters description: vrrp-mac-addr: VRRP virtual MAC address	
Event description: A virtual MAC address is adding into switch L3 table. Log Message: VRRP-5-MACL3ADD: Added a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice
Event description: A virtual MAC address is deleting from switch L3 table. Log Message: VRRP-5-MACL3DEL: Deleted a virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from L3 table Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Notice
Event description: Failed when adding a virtual MAC into switch chip L2 table. Log Message: VRRP-3-MACADDFAIL:Failed to add virtual MAC <vrrp-mac-addr> into chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behavior.	Error
Event description: Failed when deleting a virtual MAC from switch chip L2 table. Log Message: VRRP-3-MACDELFAIL:Failed to delete virtual MAC <vrrp-mac-addr> from chip L2 table. Errcode <vrrp-errcode> Parameters description: vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Errcode of VRRP protocol behaviour.	Error
Event description: Failed when adding a virtual MAC into switch L3 table. The L3 table is full. Log Message: VRRP-3-MACL3FULL: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. L3 table is full Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Error
Event description: Failed when adding a virtual MAC into switch L3 table. The port where the MAC is learned from is invalid. Log Message: VRRP-3-BADMAC: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Port <mac-port> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-port: port number of VRRP virtual MAC.	Error
Event description: Failed when adding a virtual MAC into switch L3 table. The interface where the MAC is learned from is invalid. Log Message: VRRP-3-BADINTF: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Interface <mac-intf> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address	Error

mac-intf: interface id on which VRRP virtual MAC address is based.	
Event description: Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid. Log Message: VRRP-3-BADUNIT: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into L3 table. Box id <mac-box> is invalid Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address mac-box: stacking box number of VRRP virtual MAC.	Error
Event description: Failed when adding a virtual MAC into switch chip's L3 table. Log Message: VRRP-3-MACL3ADDFAIL: Failed to add virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> into chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error
Event description: Failed when deleting a virtual MAC from switch chip's L3 table. Log Message: VRRP-3-MACL3DELFAIL: Failed to delete virtual IP <vrrp-ip-addr> MAC <vrrp-mac-addr> from chip L3 table. Errcode <vrrp-errcode> Parameters description: vrrp-ip-addr: VRRP virtual IP address vrrp-mac-addr: VRRP virtual MAC address vrrp-errcode: Err code of VRRP protocol behavior.	Error

Web

Log Description	Severity
Event description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Login failed through Web. Log Message: Login failed through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Warning
Event description: Web session timed out. Log Message: Web session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	Informational
Event description: Logout through Web. Log Message: Logout through Web (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login HTTP server.	Informational

ipaddr: The IP address of HTTP client.	
Event description: Successful login through Web (SSL). Log Message: Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Login failed through Web (SSL). Log Message: Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Warning
Event description: Web (SSL) session timed out. Log Message: Web (SSL) session timed out (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational
Event description: Logout through Web (SSL). Log Message: Logout through Web (SSL) (Username: <username>, IP: <ipaddr>). Parameters description: username: The use name that used to login SSL server. ipaddr: The IP address of SSL client.	Informational

Web-Authentication

Log Description	Severity
Event description: The log message occurs when a host passed the authentication. Log Message: Web-Authentication host login success (Username: <username>, IP: <ipaddr >, MAC: <mac-address>, <interface-id>, VID: <vlan-id>). Parameters description: username: The host username. ipaddr: The host IP address, either an IPv4 or IPv6 address. mac-address: The host MAC addresses. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Informational
Event description: The log message occurs when a host failed to pass the authentication. Log Message: Web-Authentication host login fail (Username: <username>, IP: <ipaddr >, MAC: <mac-address>, <interface-id>, VID: <vlan-id>). Parameters description: username: The host username. ipaddr: The host IP address, either an IPv4 or IPv6 address. mac-address: The host MAC addresses. interface-id: The interface on which the host is authenticated. vlan-id: The VLAN ID on which the host exists.	Critical

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the switch.

Authentication Fail

Trap Name	Description	OID
authenticationFailure	An authenticationFailure 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 the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1.5.5

CFM

Trap Name	Description	OID
dot1agCfmFaultAlarm	This trap is initiated when a connectivity defect is detected. Binding objects: (1) dot1agCfmMepHighestPrDefect	1.3.111.2.802.1.1.8.0.1

CFM Extension

Trap Name	Description	OID
swCFMExtAISOccurred	A notification is generated when local MEP enters AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.1
swCFMExtAISCleared	A notification is generated when local MEP exits AIS status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.2
swCFMExtLockOccurred	A notification is generated when local MEP enters lock status. Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	1.3.6.1.4.1.171.12.86.100.0.3
swCFMExtLockCleared	A notification is generated when local MEP exits lock status.	1.3.6.1.4.1.171.12.86.100.0

	Binding objects: (1) dot1agCfmMdIndex (2) dot1agCfmMaIndex (3) dot1agCfmMepIdentifier	.4

LACP

Trap Name	Description	OID
linkUp	A linkUp 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 some other state (but not into the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	A linkDown 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 some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

LDP

Trap Name	Description	OID
mplsLdpInitSessionThresholdExceeded	This notification is generated when the backoff is enabled, and the number of Session Initialization messages exceeds the value of the 'mplsLdpEntityInitSessionThreshold'	1.3.6.1.2.1.10.166.4.0.1
mplsLdpPathVectorLimitMismatch	This notification is sent when the'mplsLdpEntityPathVectorLimit' does NOT match the value of the 'mplsLdpPeerPathVectorLimit' for a specific Entity.	1.3.6.1.2.1.10.166.4.0.2
mplsLdpSessionUp	If this notification is sent when the value of 'mplsLdpSessionState' enters the 'operational(5)' state	1.3.6.1.2.1.10.166.4.0.3
mplsLdpSessionDown	This notification is sent when the value of 'mplsLdpSessionState' leaves the 'operational(5)' state	1.3.6.1.2.1.10.166.4.0.4

LLDP

Trap Name	Description	OID
lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. It can be utilized by an NMS to trigger LLDP remote systems table maintenance polls. Binding 1. lldpStatsRemTablesInserts 2. lldpStatsRemTablesDeletes 3. lldpStatsRemTablesDrops 4. lldpStatsRemTablesAgeouts	1.0.8802.1.1.2.0.0.1
lldpXMedTopologyChangeDetected	A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another. Binding 1. lldpRemChassisIdSubtype 2. lldpRemChassisId 3. lldpXMedRemDeviceClass	1.0.8802.1.1.2.1.5.4795.0.1

MPLS

Trap Name	Description	OID
mplsXCUp	This notification is generated when the mplsXCOperStatus object for one or more contiguous entries in the mplsXCTable is about to enter the up state from another state.	1.3.6.1.2.1.10.166.2.0.1
mplsXCDown	This notification is generated when the mplsXCOperStatus object for one or more contiguous entries in the mplsXCTable is about to enter the up state from another state.	1.3.6.1.2.1.10.166.2.0.2

MSTP

Trap Name	Description	OID
newRoot	The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17.0.1
topologyChange	A topologyChange 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. The trap is not sent if a newRoot trap is sent for the same transition. Implementation ofthis trap is optional	1.3.6.1.2.1.17.0.2

Port

Trap Name	Description	OID

linkUp	A notification is generated when port linkup. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.4
linkDown	A notification is generated when port linkdown. Binding objects: (1) ifIndex, (2) if AdminStatus (3) ifOperStatu	1.3.6.1.6.3.1.1.5.3

RMON

Trap Name	Description	OID
risingAlarm	The SNMP trap that is generated 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
fallingAlarm	The SNMP trap that is generated 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

Start

Trap Name	Description	OID
coldStart	A coldStart 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
warmStart	A warmStart 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

VPWS

Trap Name	Description	OID

pwDown	This notification is generated when the pwOperStatus object for one or more contiguous entries in the pwTable which are about to enter the down(2) or lowerLayerDown(6) state from any other state, except for transition from the notPresent(5) state.	1.3.6.1.2.1.10 .246.0.1
pwUp	This notification is generated when the pwOperStatus object for one or more contiguous entries in the pwTable which are about to enter the up(1) state from some other state except the notPresent(5) state and given that the pwDown notification issued for these entries.	1.3.6.1.2.1.10 .246.0.2
pwDeleted	This notification is generated when the PW has been deleted, i.e., when the pwRowStatus has been set destroy(6) or the PW has been deleted by a non-MIB application or due to an auto-discovery process.	1.3.6.1.2.1.10 .246.0.3

VRRP

Trap Name	Description	OID
vrrpTrapNewMaster	The newMaster trap indicates that the sending agent has transitioned to 'Master' state. Binding objects: (1) vrrpOperMasterIpAddr	1.3.6.1.2.1.68 .0.1
vrrpTrapAuthFailure	A vrrpAuthFailure trap signifies that a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type. Implementation of this trap is optional. Binding objects: (1) vrrpTrapPacketSrc (2) vrrpTrapAuthErrorType	1.3.6.1.2.1.68 .0.2

Appendix D - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the DXS-3600 is used in the following modules: Console, Telnet, SSH, Web, 802.1X, MAC-based Access Control, and WAC.

The description that follows explains the following RADIUS Attributes Assignment types:

- Privilege Level
- Ingress/Egress Bandwidth
- 802.1p Default Priority
- VLAN
- ACL

To assign the **Privilege Level** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for the bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	1	Required
Attribute-Specific Field	Used to assign the privilege level of the user to operate the switch.	Range (1-15)	Required

If the user has configured the privilege level attribute of the RADIUS server (for example, level 15) and the Console, Telnet, SSH, and Web authentication is successful, the device will assign the privilege level (according to the RADIUS server) to this access user. However, if the user does not configure the privilege level attribute and authenticates successfully, the device will not assign any privilege level to the access user. If the privilege level is configured less than the minimum supported value or greater than the maximum supported value, the privilege level will be ignored.

To assign the **Ingress/Egress Bandwidth** by the RADIUS server, the proper parameters should be configured on the RADIUS Server. The table below shows the parameters for bandwidth.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	2 (for ingress bandwidth) 3 (for egress bandwidth)	Required
Attribute-Specific Field	Used to assign the bandwidth of a port.	Unit (Kbits)	Required

If the user has configured the bandwidth attribute of the RADIUS server (for example, ingress bandwidth 1000Kbps) and 802.1X authentication is successful, the device will assign the bandwidth (according to the RADIUS server) to the port. However, if the user does not configure the bandwidth attribute and

authenticates successfully, the device will not assign any bandwidth to the port. If the bandwidth attribute is configured on the RADIUS server with a value of “0”, the effective bandwidth will be set “no_limited”, and if the bandwidth is configured less than “0” or greater than maximum supported value, the bandwidth will be ignored.

To assign the **802.1p Default Priority** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for 802.1p default priority.

The parameters of the Vendor-Specific attributes are:

Vendor-Specific Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	4	Required
Attribute-Specific Field	Used to assign the 802.1p default priority of the port.	0 to 7	Required

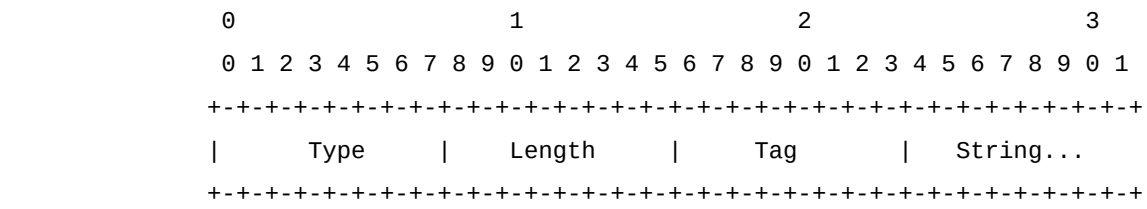
If the user has configured the 802.1p priority attribute of the RADIUS server (for example, priority 7) and the 802.1X, or MAC based authentication is successful, the device will assign the 802.1p default priority (according to the RADIUS server) to the port. However, if the user does not configure the priority attribute and authenticates successfully, the device will not assign a priority to this port. If the priority attribute is configured on the RADIUS server is a value out of range (>7), it will not be set to the device.

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.



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, or MAC based Access Control, or WAC 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.

To assign the **ACL** by the RADIUS server, the proper parameters should be configured on the RADIUS server. The table below shows the parameters for an ACL.

The parameters of the Vendor-Specific Attribute are:

RADIUS Tunnel Attribute	Description	Value	Usage
Vendor-ID	Defines the vendor.	171 (DLINK)	Required
Vendor-Type	Defines the attribute.	14 (for ACL script)	Required
Attribute-Specific Field	Used to assign the ACL script. The format is based on **Access Control List (ACL) Commands**.	ACL Script For example: **ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;**	Required

If the user has configured the ACL attribute of the RADIUS server (for example, ACL script: ip access-list a1;permit host 10.90.90.100;exit; mac access-list extended m1;permit host 00-00-00-01-90-10 any; exit;), and the 802.1X or MAC-based Access Control WAC is successful, the device will assign the ACL script according to the RADIUS server. The enter **Access-List Configuration Mode** and exit **Access-List Configuration Mode** must be a pair, otherwise the ACP script will be reject. For more information about the ACL module, please refer to **Access Control List (ACL) Commands** chapter.

Appendix E - 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), RFC 2866 RADIUS Accounting, RFC 2868 RADIUS Attributes for Tunnel Protocol Support, and RFC 2869 RADIUS Extensions.

The following table lists the IETF RADIUS attributes supported by the D-Link switch.

RADIUS Authentication Attributes:

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

RADIUS Accounting Attributes:

Number	IETF Attribute
1	User-Name
4	NAS-IP-Address
5	NAS-Port
6	Service-Type
8	Framed-IP-Address
31	Calling-Station-ID
32	NAS-Identifier
40	Acct-Status-Type
41	Acct-Delay-Time
42	Acct-Input-Octets
43	Acct-Output-Octets
44	Acct-Session-ID
45	Acct-Authentic
46	Acct-Session-Time
47	Acct-Input-Packets
48	Acct-Output-Packets
49	Acct-Terminate-Cause
52	Acct-Input-Gigawords
53	Acct-Output-Gigawords
61	NAS-Port-Type
95	NAS-IPv6-Address