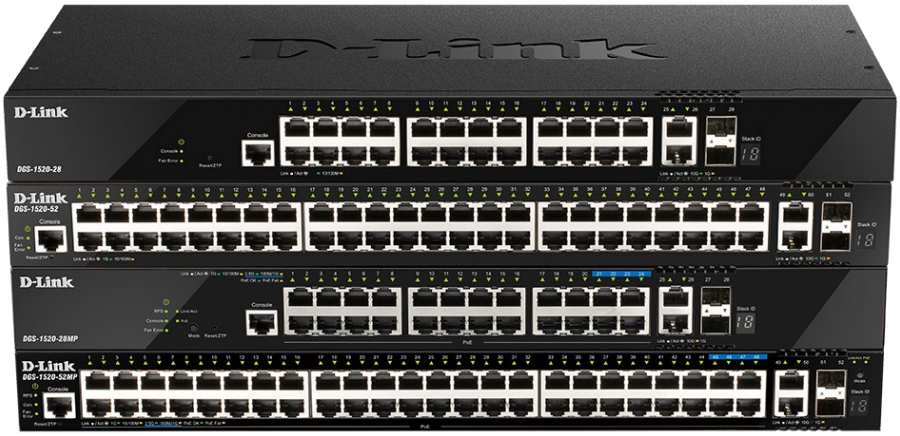
Version 1.20 | 10/18/2023



CLI Reference Guide

Gigabit Ethernet Smart Managed Switch

DGS-1520 Series

Table of Contents

1. Introduction....1
2. Basic CLI Commands....9
3. 802.1X Commands....27
4. Access Control List (ACL) Commands....41
5. Access Management Commands....73
6. ARP Spoofing Prevention Commands....99
7. Asymmetric VLAN Commands....102
8. Authentication, Authorization, and Accounting (AAA) Commands....103
9. Basic IPv4 Commands....134
10. Basic IPv6 Commands....144
11. BPDU Protection Commands....163
12. Cable Diagnostics Commands....167
13. Command Logging Commands....170
14. CPU Access Control List (ACL) Commands....171
15. CPU Port Statistics Commands....175
16. Debug Commands....178
17. DHCP Auto-Configuration Commands....188
18. DHCP Auto-Image Commands....190
19. DHCP Client Commands....193
20. DHCP Relay Commands....197
21. DHCP Server Commands....232
22. DHCP Server Screening Commands....260
23. DHCP Snooping Commands....266
24. DHCPv6 Client Commands....280
25. DHCPv6 Guard Commands....283
26. DHCPv6 Relay Commands....287
27. DHCPv6 Server Commands....308
28. Digital Diagnostics Monitoring (DDM) Commands....325
29. Distance Vector Multicast Routing Protocol (DVMRP) Commands....335
30. D-Link Discovery Protocol (DDP) Client Commands....341
31. Domain Name System (DNS) Commands....346
32. DoS Prevention Commands....352
33. Dynamic ARP Inspection Commands....356
34. Error Recovery Commands....370
35. Ethernet Ring Protection Switching (ERPS) Commands....374
36. File System Commands....397
37. Filter Database (FDB) Commands....404
38. Filter NetBIOS Commands....418
39. GARP VLAN Registration Protocol (GVRP) Commands....420
40. Gratuitous ARP Commands....429
41. Interface Commands....432
42. Internet Group Management Protocol (IGMP) Commands....458
43. Internet Group Management Protocol (IGMP) Proxy Commands....468

44. Internet Group Management Protocol (IGMP) Snooping Commands 474
45. IP Multicast (IPMC) Commands 498
46. IP Multicast Version 6 (IPMCv6) Commands 510
47. IP Source Guard Commands 516
48. IP Utility Commands 522
49. IP-MAC-Port Binding (IMPB) Commands 530
50. IPv6 Snooping Commands 534
51. IPv6 Source Guard Commands 541
52. Layer 2 Protocol Tunnel (L2PT) Commands 548
53. Link Aggregation Control Protocol (LACP) Commands 555
54. Link Layer Discovery Protocol (LLDP) Commands 562
55. Loopback Detection (LBD) Commands 590
56. Loopback Test Commands 597
57. MAC Authentication Commands 599
58. Mirror Commands 603
59. Multicast Listener Discovery (MLD) Commands 612
60. Multicast Listener Discovery (MLD) Proxy Commands 621
61. Multicast Listener Discovery (MLD) Snooping Commands 627
62. Multicast Source Discovery Protocol (MSDP) Commands 649
63. Multicast VLAN Commands 670
64. Multiple Spanning Tree Protocol (MSTP) Commands 682
65. Neighbor Discovery (ND) Inspection Commands 689
66. Network Access Authentication Commands 694
67. Network Load Balancing (NLB) Commands 708
68. Network Protocol Port Protection Commands 711
69. Network Time Protocol (NTP) Commands 713
70. Open Shortest Path First Version 2 (OSPFv2) Commands 728
71. Open Shortest Path First Version 3 (OSPFv3) Commands 786
72. Packet Debug Commands 818
73. Policy-based Routing (PBR) Commands 821
74. Port Security Commands 825
75. Power over Ethernet (PoE) Commands (DGS-1520-28MP and DGS-1520-52MP Only) 832
76. Power Saving Commands 851
77. Priority-based Flow Control (PFC) Commands 857
78. Private VLAN Commands 859
79. Protocol Independent Commands 865
80. Protocol Independent Multicast (PIM) Commands 878
81. Protocol Independent Multicast (PIM) IPv6 Commands 897
82. Protocol Independent Multicast (PIM) Snooping Commands 921
83. Quality of Service (QoS) Commands 927
84. QoS Amendment Data Center Bridge (DCB) Commands 961
85. Remote Network MONitoring (RMON) Commands 969
86. Reset Button Commands 977
87. Route Map Commands 980
88. Router Advertisement (RA) Guard Commands 995
89. Routing Information Protocol (RIP) Commands 999

90. Routing Information Protocol Next Generation (RIPng) Commands 1011
91. Safeguard Engine Commands 1024
92. Secure File Transfer Protocol (SFTP) Client Commands 1032
93. Secure File Transfer Protocol (SFTP) Server Commands 1035
94. Secure Shell (SSH) Commands 1038
95. sFlow Commands 1046
96. Simple Mail Transfer Protocol (SMTP) Commands 1052
97. Simple Network Management Protocol (SNMP) Commands 1058
98. Single IP Management (SIM) Commands 1082
99. Spanning Tree Protocol (STP) Commands 1093
100. Stacking Commands 1108
101. Storm Control Commands 1115
102. Super VLAN Commands 1120
103. Surveillance VLAN Commands 1124
104. Switch Port Commands 1130
105. System File Management Commands 1134
106. System Log Commands 1147
107. Time and SNTP Commands 1159
108. Time Range Commands 1166
109. Traffic Segmentation Commands 1169
110. Transport Layer Security (TLS) Commands 1171
111. Unicast Reverse Path Forwarding (URPF) Commands 1180
112. Virtual LAN (VLAN) Commands 1184
113. Virtual LAN (VLAN) Counter Commands 1200
114. Virtual LAN (VLAN) Tunnel Commands 1203
115. Virtual Router Redundancy Protocol (VRRP) Commands 1216
116. Virtual Router Redundancy Protocol Version 3 (VRRPv3) Commands 1229
117. Voice VLAN Commands 1237
118. Web Authentication Commands 1245
119. Weighted Random Early Detection (WRED) Commands 1250
120. Zone Defense Commands 1255
Appendix A - Password Recovery Procedure 1257
Appendix B - System Log Entries 1258
Appendix C - Trap Entries 1290
Appendix D - RADIUS Attributes Assignment 1303
Appendix E - IETF RADIUS Attributes Support 1307
Appendix F - ERPS Information 1309
Appendix G - Stacking Information 1310

1. Introduction

This manual's command descriptions are based on the software release **1.01**. The commands listed here are the subset of commands that are supported by the DGS-1520 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 DGS-1520 Series switch, which will be generally be referred to simply as the "Switch" within this manual. This manual is written in a way that assumes that you already have experience with and knowledge of Ethernet and modern networking principles for Local Area Networks.

Other Documentation

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

- *DGS-1520 Series Gigabit Ethernet Smart Managed Switch Hardware Installation Guide*
- *DGS-1520 Series Gigabit Ethernet Smart Managed Switch 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 DGS-1520-28MP switch in the DGS-1520 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.
ATTENTION: Une précaution indique un risque de dommage matériel, de blessure corporelle ou de mort.

Connecting to the Console Port

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

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

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

Command Descriptions

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

- **Description** - This is a short and concise statement describing the functionality of the command.
- **Syntax** - The precise form to use when entering and issuing the command.
- **Parameters** - A table where each row describes the optional or required parameters, and their use, that can be issued with the command.
- **Default** - If the command sets a configuration value or administrative state of the Switch then any default settings (i.e. without issuing the command) of the configuration is shown here.
- **Command Mode** - The mode in which the command can be issued. These modes are described in the section titled “Command Modes” below.
- **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 three 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. This user account level can only show information not security-related.
- **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 / Operator level	For changing local and global terminal settings, monitoring, and performing certain system administration tasks. Except for security related information, this level can perform system administration tasks.
Privileged EXEC Mode / Administrator level	This level is identical to privileged EXEC mode at the operator 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.

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 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 log into 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 log into 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 to the entire switch. The global configuration mode can be accessed through advanced user, power user, operator or administrator level user accounts. However, security related settings are not accessible through advanced user, power user or operator user accounts. In addition to applying global settings to the entire switch, the user can also access other sub-configuration modes. In order to access the global configuration mode, 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.

Creating a User Account

You can create different user account for various levels. This section will assist a user with creating a user account by means of the Command Line Interface.



NOTE: By default, one user account is already configured on the Switch. Both the username and password for this account is admin, and the privilege level is 15.

Observe the following example.

```
Switch#enable
Switch#configure terminal
Switch(config)#username user1 password 1234
Switch(config)#username user1 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 **enable** command to access the Privileged EXEC Mode.
- After accessing the Privileged EXEC Mode, we entered the **configure terminal** command to access the Global Configuration Mode. The **username** command can be used in the Global Configuration Mode.
- The **username user1 password 1234** command creates a user account with the username of *user1* and a password of *1234*.
- The **username user1 privilege 15** command assigns a privilege level value of 15 to the user account admin.
- The **line console** command allows us to access the console interface's Line Configuration Mode.
- The **login local** command tells 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 has rebooted, or after the users log out and back in, the newly created username and password must be entered to access the CLI interface again, as seen below.

```
                    DGS-1520-28MP Gigabit Ethernet Smart Managed Switch

                                  Command Line Interface
                                 Firmware: Build 1.01.004
               Copyright(C) 2022 D-Link Corporation. All rights reserved.

User Access Verification

Username:user1
Password:****

Switch#
```

Interface Notation

When configuring 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 will 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 will change the speed to 1 Gbps, using the **speed 1000** command.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
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, 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 DGS-1520 Series switch does not support any open modules slots, thus this parameter will always be 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 users issue a command that the Switch does not recognize, error messages will be generated to assist users with basic information about the mistake that was made. A list of possible error messages are found in the table below.

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

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

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

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

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

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

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

Editing Features

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

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

Display Result Output Modifiers

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

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

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

```
Switch#show running-config | begin interface ethernet 1/0/27
interface ethernet 1/0/27
!
interface ethernet 1/0/28
!
interface Vlan1
!
interface Null0
!
ntp access-group default nomodify noquery
!
!
end


Switch#
```

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

```
Switch#show running-config | include line
line console
line telnet
line ssh


Switch#
```

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

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

Current configuration : 1502 bytes


line console
line telnet
line ssh
network-protocol-port protect tcp
network-protocol-port protect udp
configure terminal
end
interface Mgmt0
interface ethernet 1/0/1
interface ethernet 1/0/2
interface ethernet 1/0/3
interface ethernet 1/0/4
interface ethernet 1/0/5
interface ethernet 1/0/6
interface ethernet 1/0/7
interface ethernet 1/0/8
interface ethernet 1/0/9
interface ethernet 1/0/10
interface ethernet 1/0/11
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

2. Basic CLI Commands

2-1 help

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

help

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

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

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

Switch#
```

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

```
Switch#re?
reboot              rename              renew               reset

Switch#re
```

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

```
Switch#stack ?
  <1-8>      Specifies current box ID
  bandwidth  Stacking port bandwidth
  preempt    Preempt the master role play
  <cr>

Switch#stack
```

2-2 enable

This command is used to change the privilege level of the active CLI login session.

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

Parameters

PRIVILEGE-LEVEL	(Optional) Specifies the privilege level. The range is from 1 to 15. If this parameter is not specified, privilege level 15 will be used.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If the privileged level requires a password, enter it in the field provided. Only three attempts are allowed. Failure to access this level returns the user to the current level.

Example

This example shows how to change the privilege level of the active CLI login session to privilege level 12.

```
Switch#show privilege

Current privilege level is 2

Switch#enable 15
password:******
Switch#show privilege

Current privilege level is 15

Switch#
```

2-3 disable

This command is used to change the privilege level of the active CLI login session to a lower privilege level.

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

Parameters

PRIVILEGE-LEVEL	(Optional) Specifies the privilege level. The range is from 1 to 15. If this parameter is not specified, privilege level 1 will be used.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to change the privilege level of the active CLI login session to a lower privilege level.

Example

This example shows how to change the privilege level of the active CLI login session to privilege level 1.

```
Switch#show privilege

Current privilege level is 15

Switch#disable 1
Switch>show privilege

Current privilege level is 1

Switch>
```

2-4 configure terminal

This command is used to enter the Global Configuration Mode.

configure terminal

Parameters

None.

Default

None

Command Mode

Privileged 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 the 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to change the login account. Three attempts are allowed to log into 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 this command to disable the login.

login [local]

no login

Parameters

local	(Optional) Specifies that the line login method will be local.

Default

By default, the **console**, **Telnet**, and **SSH** line use the **login local** method (username and password).

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 **password** command, the user will 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
- 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 are ignored. Enter the details at Level 1.
    - When the **username and password** option is selected, enter the username and password configured 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/Privileged 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 log out.

```
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

User/Privileged EXEC Mode.

Any Configuration Mode.

Command Default Level

Level: 1.

Usage Guideline

Executing this command will return access to the highest mode in the CLI hierarchy.

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 eth1/0/1
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 Privileged EXEC Mode, executing the exit command logs you out of the current session.

exit

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

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 Privileged EXEC Mode, this command will log out 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

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

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

Example

This example shows how to display the command buffer history.

```
Switch#show history

 help
 history

Switch#
```

2-11 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 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:

- Updates an existing user account by entering the username of an existing user and its new password, or adds a new user account with privilege level 15. The new user account cannot be created if the maximum number of user accounts is exceeded.
- Updates the enabled password for the administrator-privileged level.
- Disables 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.

The updated setting will be saved in the running configuration file. Before the reload is executed, the Switch will prompt user if saving the running configuration as the startup configuration, or prompt user if clearing the startup configuration when clear startup-config option is selected.

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 detailed fan status.

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

Default

None.

Command Mode

User/Privileged EXEC 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         23C/11~79C
Status code: * temperature is out of threshold range

Detail Fan Status:
-------------------------------------------------------------
Unit 1:
  Right Fan 1 (OK)     Right Fan 2 (OK)     Right Fan 3 (OK)
  Right Fan 4 (OK)

Detail Power Status:
Unit    Power Module      Power Status
-----   ----------------  -------------
1       Power 1           In-operation
1       Power 2           Empty

Switch#
```

Display Parameters

Power Module	**Power 1:** This represents the AC power. **Power 2:** This represents the RPS.
Power status	**in-operation:** The power rectifier is in normal operation. **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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show unit

Unit: 1
Model Descr: 20 ports GE PoE + 4 ports 2.5 GE PoE + 2 10GE ports + 2 SFP+ Smart Managed Sw
itch
Model Name: DGS-1520-28MP
Serial-Number: DGS1520-28MPA
Status: OK
Up Time: 0DT1H39M47S
DRAM      524288 K total,   223786 K used,   300502 K free
FLASH      60823 K total,    59384 K used,     1439 K free

Switch#
```

2-14 show cpu utilization

This command is used to display the CPU utilization information.

show cpu utilization [history {15_minute [slot *INDEX***] | 1_day [slot** *INDEX***]}]**

Parameters

history	(Optional) Specifies to display the historical CPU utilization information.
15_minute	(Optional) Specifies to display the 15-minute based statistics count.

1_day	(Optional) Specifies to display the daily based statistics count.
slot *INDEX*	(Optional) Specifies the slot number to be displayed. For 15-minute based statistics count, the range is from 1 to 5. For 1-day based statistics count, the range is from 1 to 2. If no slot is specified, information of all slots will be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the CPU utilization information of the Switch in 5 second, 1 minute, and 5 minute intervals.

There are two kinds of statistics offered for the historical utilization statistics: 15-minute based and 1-day based. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago, and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

Example

This example shows how to display the CPU utilization information.

```
Switch#show cpu utilization

CPU Utilization

Five seconds -  14 %         One minute -  14 %         Five minutes -  14 %


Switch#
```

This example shows how to display the CPU utilization history in 15-minute slots.

```
Switch#show cpu utilization history 15_minute

CPU Utilization:
12 Dec 2019  10:00:08 - 12 Dec 2019  09:45:08  : 5   %
12 Dec 2019  09:45:08 - 12 Dec 2019  09:30:08  : 6   %
12 Dec 2019  09:30:08 - 12 Dec 2019  09:15:08  : 6   %
12 Dec 2019  09:15:08 - 12 Dec 2019  09:00:08  : 6   %
12 Dec 2019  09:00:08 - 12 Dec 2019  08:45:08  : 9   %

Switch#
```

2-15 show version

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

show version

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show version

System MAC Address: 80-26-89-15-28-00

Unit ID    Module Name                    Versions
-------  ---------------------------  --------------------
   1      DGS-1520-28MP                H/W:A1
                                       Bootloader:1.00.011
                                       Runtime:1.01.004


Switch#
```

2-16 snmp-server enable traps environment

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

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

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

Parameters

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

Default

By default, all environment device traps are disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Example

This example shows how to enable the environment trap status.

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

2-17 environment temperature threshold

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

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. The value is 1.
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

By default, the normal range is the same as the operation range.

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)#
```

2-18 show memory utilization

This command is used to display the memory utilization information.

show memory utilization [history {15_minute [slot *INDEX***] | 1_day [slot** *INDEX***]}]**

Parameters

history	(Optional) Specifies to display the historical memory utilization information.
15_minute	(Optional) Specifies to display the 15-minute based statistics count.
1_day	(Optional) Specifies to display the daily based statistics count.
slot *INDEX*	(Optional) Specifies the slot number to be displayed. For 15-minute based statistics count, the range is from 1 to 5. For 1-day based statistics count, the range is from 1 to 2. If no slot is specified, information of all slots will be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the memory utilization information of the Switch including DRAM and flash.

There are two kinds of statistics offered for the historical utilization statistics: 15-minute based and 1-day based. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

Historical memory utilization information only displays DRAM memory information.

Example

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

```
SSwitch#show memory utilization

Unit: 1
DRAM      524288 K total,   223606 K used,   300682 K free
FLASH      60823 K total,    44847 K used,    15976 K free

Switch#
```

This example shows how to display the historical memory utilization in 15-minute slots.

```
Switch#show memory utilization history 15_minute

Unit 1 DRAM Utilization:
1  Jan 2019  01:24:25 - 1  Jan 2019  01:09:25  : 42  %
1  Jan 2019  01:09:25 - 1  Jan 2019  00:54:25  : 42  %
1  Jan 2019  00:54:25 - 1  Jan 2019  00:39:25  : 42  %
1  Jan 2019  00:39:25 - 1  Jan 2019  00:24:25  : 42  %
1  Jan 2019  00:24:25 - 1  Jan 2019  00:09:25  : 42  %

Switch#
```

2-19 privilege

This command is used to configure the execution rights of a command string to a privilege level. Use the **no** form of this command to revert the command string to the default privilege level.

privilege *MODE* **{level** *PRIVILEGE-LEVEL* **| reset }** *COMMAND-STRING*

no privilege *MODE COMMAND-STRING*

Parameters

MODE	Specifies the command mode of the command.
level *PRIVILEGE-LEVEL*	Specifies the level of the execution right. The value is from 1 to 15.
reset	Specifies to revert the command to the default privilege level.
COMMAND-STRING	Specifies the command to be changed.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to configure the execution rights of a command string to a privilege level. When this command is used, the command string used must exist at current command level. When more than one command

begins with the command string specified, all of the commands starting with that command string will be changed to the specified command level.

Example

This example shows how to configure the **configure terminal** command string as a level 12 command.

```
Switch#enable 15
Switch#configure terminal
Switch(config)#privilege exec level 12 configure terminal
Switch(config)#
```

2-20 show privilege

This command is used to display the current privilege level.

show privilege

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the current privilege level.

Example

This example shows how to display the current privilege level.

```
Switch#show privilege

Current privilege level is 15

Switch#
```

3. 802.1X Commands

3-1 clear dot1x counters

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

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

Parameters

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

Default

None.

Command Mode

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 port 1.

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

3-2 dot1x control-direction

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

dot1x control-direction {both | in}

no dot1x control-direction

Parameters

both	Specifies to enable bidirectional control for the port.

in	Specifies to enable in direction control for the port.

Default

By default, the bidirectional mode is used.

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

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

Example

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

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

3-3 dot1x default

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

dot1x default

Parameters

None.

Default

IEEE 802.1X authentication is disabled.

Control direction is bidirectional mode.

Port control is auto.

Forward PDU on port is disabled.

Maximum request is 2 times.

Server timer is 30 seconds.

Supplicant timer is 30 seconds.

Transmit interval is 30 seconds.

Command Mode

Interface Configuration Mode.

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. This command is only available for physical port interfaces.

Example

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

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

3-4 dot1x port-control

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

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

no dot1x port-control

Parameters

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

Default

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

Command Mode

Interface Configuration Mode.

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

Example

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

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

3-5 dot1x forward-pdu

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

dot1x forward-pdu

no dot1x forward-pdu

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

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

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

Example

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

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

3-7 dot1x max-req

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

dot1x max-req *TIMES*

no dot1x max-req

Parameters

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

Default

By default, this value is 2.

Command Mode

Interface Configuration Mode.

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 port 1 to be 3.

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

3-8 dot1x pae authenticator

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

dot1x pae authenticator

no dot1x pae authenticator

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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 port 1 as an IEEE 802.1X PAE authenticator.

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

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

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

3-9 dot1x re-authenticate

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

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

Parameters

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

Default

None.

Command Mode

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.

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

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

Example

This example shows how to re-authenticate port 1.

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

3-10 dot1x system-auth-control

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

dot1x system-auth-control

no dot1x system-auth-control

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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 this command to revert to the default settings.

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

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

Parameters

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

Default

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

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

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

Command Mode

Interface Configuration Mode.

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 port 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 this parameter is not specified, the global configuration will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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
Trap State              : Enabled

Switch#
```

This example shows how to display the dot1X configuration on port 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        : Enabled

Switch#
```

3-13 show dot1x diagnostics

This command is used to display IEEE 802.1X diagnostics.

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

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces. If this parameter is not specified, information about all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display 802.1X diagnostics. If no optional parameter is specified, information of all interfaces will be displayed.

Example

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

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

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

Switch#
```

3-14 show dot1x statistics

This command is used to display IEEE 802.1X statistics.

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

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces. If this parameter is not specified, information about all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display 802.1X statistics. If no optional parameter is specified, information of all interfaces will be displayed.

Example

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

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

 eth1/0/1 dot1x statistics information:
 EAPOL Frames RX                      : 2
 EAPOL Frames TX                      : 3
 EAPOL-Start Frames RX                : 0
 EAPOL-Req/Id Frames TX               : 1
 EAPOL-Logoff Frames RX               : 0
 EAPOL-Req Frames TX                  : 1
 EAPOL-Resp/Id Frames RX              : 1
 EAPOL-Resp Frames RX                 : 1
 Invalid EAPOL Frames RX              : 0
 EAP-Length Error Frames RX           : 0
 Last EAPOL Frame Version             : 1
 Last EAPOL Frame Source              : 00-0D-88-11-8B-6A

Switch#
```

3-15 show dot1x session-statistics

This command is used to display IEEE 802.1X session statistics.

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

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display the dot1x diagnostics on the specified interface or range of interfaces. If this parameter is not specified, information about all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command can be used to display 802.1X session statistics. If no optional parameter is specified, information of all interfaces will be displayed.

Example

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

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

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

Switch#
```

3-16 snmp-server enable traps dot1x

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

snmp-server enable traps dot1x

no snmp-server enable traps dot1x

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Example

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

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

4. Access Control List (ACL) Commands

4-1 access-list resequence

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

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

no access-list resequence

Parameters

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

Default

The default start sequence number is 10.

The default increment is 10.

Command Mode

Global Configuration Mode.

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, there will be no re-sequencing.

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

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

Example

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

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

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

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

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

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

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

Switch#
```

4-2 acl-hardware-counter

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

acl-hardware-counter {access-group {*ACCESS-LIST-NAME* **|** *ACCESS-LIST-NUMBER***} | 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 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** form of this command to revert to the default setting.

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, 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 access list: ext_mac(ID: 7999)
  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 access list:  ext_mac(ID: 7999)
  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#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** form of this 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 port 2 to filter the incoming packets.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#expert access-group exp_acl in

 PROMPT: The remaining applicable EXPERT related access entries are 1664, remaining range
entries are 32.
Switch(config-if)#
```

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** form of this 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	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)#
```

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	(Optional) Specifies that the IP access list will be applied to check packets in the ingress direction. If the direction is not specified, **in** is used.
out	(Optional) Specifies that the IP access list will be applied to check packets in the egress direction.

Default

None.

Command Mode

Interface Configuration Mode.

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

Example

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

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

 PROMPT: The remaining applicable IP related access entries are 3327, remaining range entries are 32.
Switch(config-if)#
```

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** form of this command to remove an IP access list.

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

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

Parameters

extended	(Optional) Specifies that the IP access list is the extended IP access list, and more fields can be chosen for the filter. If the parameter is not specified, the IP access list is the standard IP access list.
NAME	Specifies the name of the IP access list to be configured. The maximum length is 32 characters. The first character must be a letter.
NUMBER	Specifies the ID number of the IP access list. For standard IP access lists, this value is from 1 to 1999. For extended IP access lists, this value is from 2000 to 3999.

Default

None.

Command Mode

Global Configuration Mode.

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
Switch(config-ip-ext-acl)#permit tcp any 10.20.0.0 0.0.255.255
Switch(config-ip-ext-acl)#exit
Switch(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** form of this command to remove an IPv6 access list.

ipv6 access-group {*NAME* **|** *NUMBER***} [in | out]**

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

Parameters

NAME	Specifies the name of the IPv6 access list to be applied.
NUMBER	Specifies the number of the IPv6 access list to be applied.
in	(Optional) Specifies that the IPv6 access list will be applied to check in the ingress direction. If the direction is not specified, **in** is used.
out	(Optional) Specifies that the IPv6 access list will be applied to check 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, an error message will be displayed.

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

Example

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

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

 PROMPT: The remaining applicable IPv6 related access entries are 767, remaining range entries are 32.
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

extended	(Optional) Specifies that the IPv6 access list is the extended IPv6 access list, and more fields can be chosen for the filter. If the parameter is not specified, the IPv6 access list is the standard IPv6 access list.

NAME	Specifies the name of the IPv6 access list to be configured. The maximum length is 32 characters.
NUMBER	Specifies the ID number of the IPv6 access list. For standard IPv6 access lists, this value is from 11000 to 12999. For extended IPv6 access lists, this value is from 13000 to 14999.

Default

None.

Command Mode

Global Configuration Mode.

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
Switch(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
Switch(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** form of this command to delete the remarks.

list-remark *TEXT*

no list-remark

Parameters

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

Default

None.

Command Mode

Access-list Configuration Mode.

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

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

Switch#
```

4-12 mac access-group

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

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

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

Parameters

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

Example

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

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

 PROMPT: The remaining applicable MAC related access entries are 1535, remaining range entries are 32.
Switch(config-if)#
```

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** form of this command to delete a MAC access list.

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

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

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

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. Use the **no** form of this command to remove the matched 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). The IP sub-map only checks IP packets. Newer commands will overwrite the previous settings.

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 access list:  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. Use the **no** form of this command to remove the matched 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). The IPv6 sub-map only checks IPv6 packets. Newer commands will overwrite the previous settings.

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 access list:  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. Use the **no** form of this command to remove the matched 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). The MAC sub-map only checks non-IP packets. Newer commands will overwrite the previous settings.

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

Switch#
```

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

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

Extended Expert ACL:

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu}** *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* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [fragments] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **| mask** *PORT MASK***] {***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* **| mask** *PORT MASK***] [***TCP-FLAG***] [cos** *OUTER-COS* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **| mask** *PORT MASK***] {***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* **| mask** *PORT MASK***] [cos** *OUTER-COS* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} 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* **[***MASK***] [inner** *INNER-COS* **[***MASK***]]] [{vlan** *OUTER-VLAN* **[***MASK***] | vlan-range** *MIN-VID MAX-VID***} [inner** *INNER-VLAN* **[***MASK***]]] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [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.
PROTOCOL	(Optional) Specifies the IP protocol ID or one of the following protocol names. Available protocol names are **eigrp**, **esp**, **gre**, **igmp**, **ospf**, **pim**, **vrrp**, **pcp** and **ipinip**. If the protocol ID is specified, the *MASK* (0x0-0xff) parameter is optional. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
cos *OUTER-COS*	(Optional) Specifies the outer priority value. This value must be between 0 and 7.
MASK	(Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
inner *INNER-COS*	(Optional) Specifies the inner priority value. This value must be between 0 and 7.
MASK	(Optional) Specifies the inner priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
vlan *OUTER-VLAN*	(Optional) Specifies the outer VLAN ID.
MASK	(Optional) Specifies the outer VLAN ID mask (0x0-0xfff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
vlan-range *MIN-VID MAX-VID*	(Optional) Specifies a range of VLANs.
inner *INNER-VLAN*	(Optional) Specifies the inner VLAN ID.
MASK	(Optional) Specifies the inner VLAN ID mask (0x0-0xfff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
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.
host *SRC-IP-ADDR*	Specifies a specific source host IP address.
SRC-IP-ADDR SRC-IP-WILDCARD	Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-IP-ADDR*	Specifies a specific destination host IP address.
DST-IP-ADDR DST-IP-WILDCARD	Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
precedence *PRECEDENCE*	(Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7.
MASK	(Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.

MASK	(Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
dscp *DSCP*	(Optional) Specifies the matching DSCP code in the IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
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 falling within the specified range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
fragments	(Optional) Specifies the packet fragment's filtering.
time-range *PROFILE-NAME*	(Optional) Specifies the name of 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 **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the 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 be more difficult 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 | deny-cpu (expert access-list)** command is removed, the user can still use the *PROTOCOL* option of the **permit | deny | deny-cpu (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)#
```

4-18 permit | deny | deny-cpu (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 | deny-cpu} tcp {any | host** *SRC-IP-ADDR* **|** *SRC-IP-ADDR SRC-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IP-ADDR* **|** *DST-IP-ADDR DST-IP-WILDCARD***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [[precedence** *PRECEDENCE* **[***MASK***]] [tos** *TOS* **[***MASK***]] | dscp** *DSCP* **[***MASK***]] [time-range** *PROFILE-NAME***]**

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

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

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

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

Standard IP Access List:

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

no *SEQUENCE-NUMBER*

Parameters

SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source IP address or any destination IP address.
host *SRC-IP-ADDR*	Specifies a specific source host IP address.
SRC-IP-ADDR SRC-IP-WILDCARD	Specifies a group of source IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-IP-ADDR*	Specifies a specific destination host IP address.
DST-IP-ADDR DST-IP-WILDCARD	Specifies a group of destination IP addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
precedence *PRECEDENCE*	(Optional) Specifies that packets can be filtered by precedence level, as specified by a number from 0 to 7.
MASK	(Optional) Specifies the precedence mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
dscp *DSCP*	(Optional) Specifies the matching DSCP code in the IP header. The range is from 0 to 63, or select the following DSCP name: af11 - 001010, af12 -001100, af13 - 001110, af21 - 010010, af22 - 010100, af23 - 010110, af31 - 011010, af32 - 011100, af33 - 011110, af41 - 100010, af42 - 100100, af43 - 100110, cs1 - 001000, cs2 - 010000, cs3 - 011000, cs4 - 100000, cs5 - 101000, cs6 - 110000, cs7 - 111000, default - 000000, ef – 101110.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
tos *TOS*	(Optional) Specifies that packets can be filtered by type of service level, as specified by a number from 0 to 15.
MASK	(Optional) Specifies the ToS mask (0x0-0xf). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if falling within the specified range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
fragments	(Optional) Specifies the packet fragment's filtering
time-range *PROFILE-NAME*	(Optional) Specifies the name of the time period profile associated with the access list delineating its activation period.
tcp, udp, igmp, ipinip, gre, esp, eigrp, ospf, pcp, pim, vrrp	Specifies Layer 4 protocols.
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255. Enter 255 to permit/deny any protocol ID.

MASK	(Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.
ICMP-CODE	(Optional) Specifies the ICMP message code. The valid number for the message code is from 0 to 255.
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The pre-defined parameters are available for selection: administratively-prohibited,alternate-address,conversion-error,host-prohibited,net-prohibited,echo,echo-reply,pointer-indicates-error,host-isolated,host-precedence-violation,host-redirect,host-tos-redirect,host-tos-unreachable,host-unknown,host-unreachable, information-reply,information-request,mask-reply,mask-request,mobile-redirect,net-redirect,net-tos-redirect,net-tos-unreachable, net-unreachable,net-unknown,bad-length,option-missing,packet-fragment,parameter-problem,port-unreachable,precedence-cutoff, protocol-unreachable,reassembly-timeout,redirect-message,router-advertisement,router-solicitation,source-quench,source-route-failed, time-exceeded,timestamp-reply,timestamp-request,traceroute,ttl-expired,unreachable.

Default

None.

Command Mode

IP Access-list Configuration Mode.

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 **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the 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 be more difficult 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 for network 10.20.0.0, permit TCP packets destined for host 10.100.1.2, permit all TCP packets go to TCP destination port 80 and permit all ICMP packets.

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

This example shows how to create two entries for an IP standard access list, named “std-acl”. These entries are: permit IP packets destined for network 10.20.0.0, permit IP packets destined for 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 | deny-cpu (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 | deny-cpu} tcp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [{eq | lt | gt | neq}** *PORT* **| range** *MIN-PORT MAX-PORT* **| mask** *PORT MASK***] [***TCP-FLAG***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

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

[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} icmp {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [***ICMP-TYPE***] [***ICMP-CODE***] |** *ICMP-MESSAGE***] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[***MASK***]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**
[*SEQUENCE-NUMBER***] {permit | deny | deny-cpu} {esp | pcp | sctp | protocol-id** *PROTOCOL-ID* **[***MASK***]} {any | host** *SRC-IPV6-ADDR* **|** *SRC-IPV6-ADDRIPREFIX-LENGTH***} {any | host** *DST-IPV6-ADDR* **|** *DST-IPV6-ADDRIPREFIX-LENGTH***} [fragments] [dscp** *VALUE* **[***MASK***] | traffic-class** *VALUE* **[MA***S***K]] [flow-label** *FLOW-LABEL* **[***MASK***]] [time-range** *PROFILE-NAME***]**

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

Standard IPv6 Access List:

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

no *SEQUENCE-NUMBER*

Parameters

SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source IPv6 address or any destination IPv6 address.
host *SRC-IPV6-ADDR*	Specifies a specific source host IPv6 address.
SRC-IPV6-ADDR/PREFIX-LENGTH	Specifies a source IPv6 network.
host *DST-IPV6-ADDR*	Specifies a specific destination host IPv6 address.
DST-IPV6-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.
MASK	(Optional) Specifies the DSCP mask (0x0-0x3f). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
traffic-class *VALUE*	(Optional) Specifies the matching traffic class value in the IPv6 header. The range is from 0 to 255.
MASK	(Optional) Specifies the traffic class mask (0x0-0xff). If this parameter is not specified, 0xff is used.
lt *PORT*	(Optional) Specifies to match if less than the specified port number.
gt *PORT*	(Optional) Specifies to match if greater than the specified port number.
eq *PORT*	(Optional) Specifies to match if equal to the specified port number.
neq *PORT*	(Optional) Specifies to match if not equal to the specified port number.
range *MIN-PORT MAX-PORT*	(Optional) Specifies to match if falling within the specified range of ports.
mask *PORT MASK*	(Optional) Specifies to match ports defined by the mask. The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
PROTOCOL-ID	(Optional) Specifies the protocol ID. The valid value is from 0 to 255.
MASK	(Optional) Specifies the protocol ID mask (0x0-0xff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number of the message type is from 0 to 255.
ICMP-CODE	(Optional) Specifies the ICMP message code. The valid number of the code type is from 0 to 255.
ICMP-MESSAGE	(Optional) Specifies the ICMP message. The following pre-defined parameters are available for selection: beyond-scope, destination-unreachable, echo-reply, echo-request, erroneous_header, hop-limit, multicast-listener-query, multicast-listener-done, multicast-listener-report, nd-na, nd-ns, next-header, no-admin, no-route, packet-too-big, parameter-option, parameter-problem, port-unreachable, reassembly-timeout, redirect, renum-command, renum-result, renum-seq-number, router-advertisement, router-renumbering, router-solicitation, time-exceeded, unreachable.

TCP-FLAG	(Optional) Specifies the TCP flag fields and the specified TCP header bits called **ack** (acknowledge), **fin** (finish), **psh** (push), **rst** (reset), **syn** (synchronize), or **urg** (urgent).
flow-label *FLOW-LABEL*	(Optional) Specifies the flow label value, within the range of 0 to 1048575.
MASK	(Optional) Specifies the flow label mask (0x0-0xfffff). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
fragments	(Optional) Specifies the packet fragment's filtering
time-range *PROFILE-NAME*	(Optional) Specifies the name of time period profile associated with the access list delineating its activation period.

Default

None.

Command Mode

IPv6 Access-list Configuration Mode.

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 **access-list resequence** command to change the start sequence number and the increment number of entries for the specified access list. After the command is applied, new entries without any specified sequence number will be assigned a number based on the 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 be more difficult 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 for network ff02::0:2/16, permit TCP packets destined for 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 for network ff02::0:2/16, and permit IP packets destined for 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 | deny-cpu (mac access-list)

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

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

no *SEQUENCE-NUMBER*

Parameters

SEQUENCE-NUMBER	Specifies the sequence number. The range is from 1 to 65535. The lower the number is, the higher the priority of the permit/deny rule.
any	Specifies any source MAC address or any destination MAC address.
host *SRC-MAC-ADDR*	Specifies a specific source host MAC address.
SRC-MAC-ADDR SRC-MAC-WILDCARD	Specifies a group of source MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
host *DST-MAC-ADDR*	Specifies a specific destination host MAC address.
DST-MAC-ADDR DST-MAC-WILDCARD	Specifies a group of destination MAC addresses by using a wildcard bitmap. The bit corresponding to the bit value 1 will be ignored. The bit corresponding to the bit value 0 will be checked.
ethernet-type *TYPE MASK*	(Optional) Specifies that the Ethernet type which is a hexadecimal number from 0 to FFFF or the name of an Ethernet type which can be one of the following: aarp, appletalk, decnet-iv, etype-6000, etype-8042, lat, lavc-sca, mop-console, mop-dump, vines-echo, vines-ip, xns-idp, or arp.
cos *VALUE*	(Optional) Specifies the priority value of 0 to 7.
MASK	(Optional) Specifies the outer priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
inner *INNER-COS*	(Optional) Specifies the inner priority value. The range is from 0 to 7.
MASK	(Optional) Specifies the inner priority mask (0x0-0x7). The bit corresponding to the bit value 0 will be ignored. The bit corresponding to the bit value 1 will be checked.
vlan *VLAN-ID*	(Optional) Specifies the VLAN-ID.
MASK	(Optional) Specifies the outer VLAN ID mask (0x0-0x0fff). If this parameter is not specified, 0x0fff is used.
vlan-range *MIN-VID MAX-VID*	(Optional) Specifies a range of VLANs.
inner *INNER-VLAN*	(Optional) Specifies the inner VLAN ID.

MASK	(Optional) Specifies the inner VLAN ID mask (0x0-0x0fff). If this parameter is not specified, 0x0fff is used.
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/Privileged EXEC 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.
arp	(Optional) Specifies to display the ARP access list.
NAME	(Optional) Specifies to the name of the access list to be displayed.
NUMBER	(Optional) Specifies to the ID of the access list to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

This example shows how to display all access lists.

```
Switch#show access-list

Access-List-Name                                Type
----------------------------------------   ---------------
Strict-Control(ID: 3999)                   ip ext-acl
daily-profile(ID: 7999)                    mac ext-acl
exp_acl(ID: 9999)                          expert ext-acl
ip6-control(ID: 14999)                     ipv6 ext-acl

Total Entries: 4


Switch#
```

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

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

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

Switch#
```

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

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

Extended IP access simple-ip-acl(ID:3994)
    10 permit tcp any 10.20.0.0 0.0.255.255  (Ing: 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): eth1/0/5-1/0/8
 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/Privileged EXEC 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

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

Default

None.

Command Mode

User/Privileged EXEC 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. Use the **no** form of this command 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, 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** form of this 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-list *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)#
```

5. Access Management Commands

5-1 access class

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

access-class *IP-ACL*

no access-class *IP-ACL*

Parameters

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

Default

None.

Command Mode

Line Configuration Mode.

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** form of this command to revert to the default setting.

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, 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 #
Enter TEXT message.  End with the character '#'.
Enter Command Line Interface
#
Switch(config)#
```

5-3 do

This command is used to execute commands originally in the User/Privileged EXEC mode in the Global Configuration Mode or other configuration modes.

do *COMMAND*

Parameters

None.

Default

None.

Command Mode

Any Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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



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

Example

This example shows how to execute the **show privilege** command in the Global Configuration Mode.

```
Switch#configure terminal
Switch(config)#do show privilege

Current privilege level is 15

Switch(config)#
```

5-4 prompt

This command is used to customize the CLI prompt. Use the **no** form of this command to revert to the 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** - Specifies to encode the SNMP server name. • **%s** - Specifies to have space.

- **%%** - Specifies to encode the % symbol.

Default

By default, the string encodes the SNMP server name.

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 prompt can only display up to 15 characters. 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)#
```

5-5 enable password

This command is used to setup enable password to enter different privileged levels. Use the **no** form of this command to return the password to the empty string.

enable password [level *PRIVILEGE-LEVEL***] [0 | 7 | 15]** *PASSWORD*

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

Parameters

level *PRIVILEGE-LEVEL*	(Optional) 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	(Optional) 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 is not specified, the syntax remains plain text.
7	(Optional) 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.
15	(Optional) Specifies the password in the encrypted form based on MD5. The password length is fixed at 31 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

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(config)#
```

5-6 ip http server

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

ip http server

no ip http server

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Example

This example shows how to enable the HTTP server.

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

5-7 ip http secure-server

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

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

no ip http secure-server

Parameters

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

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables the HTTPS server function and uses the specified SSL service policy for HTTPS. When no optional parameter is specified, a built-in local certificate will be used for HTTPS.

Example

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

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

5-8 ip {http | https} access-class

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

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

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

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

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 226.1.1.1 is allowed to access the server.

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

5-9 ip http service-port

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

ip http service-port *TCP-PORT*

no ip http service-port

Parameters

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

Default

By default, this port number is 80.

Command Mode

Global Configuration Mode.

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)#
```

5-10 ip http timeout-policy idle

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

ip http timeout-policy idle *INT*

no ip http timeout-policy idle

Parameters

INT	Specifies the idle timeout value. The valid range is from 60 to 36000 seconds.

Default

By default, this value is 180 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command configures the idle timeout value of the HTTP server connection.

Example

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

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

5-11 ip telnet server

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

ip telnet server

no ip telnet server

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables or disables the Telnet server.

Example

This example shows how to enable the Telnet server.

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

5-12 ip telnet service port

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

ip telnet service-port *TCP-PORT*

no ip telnet service-port

Parameters

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

Default

By default, this 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)#
```

5-13 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)#
```

5-14 service password-recovery

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

5-15 service password-encryption

This command is used to enable the encryption of the password before stored in the configuration file. Use the **no** form of this command to disable the encryption.

service password-encryption [7 | 15]

no service password-encryption

Parameters

7	(Optional) Specifies the password in the encryption form based on SHA-I. If no parameter is specified, this is the default form.
15	(Optional) Specifies the password in the encrypted form based on MD5.

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 **service 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)#
```

5-16 show terminal

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

show terminal

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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: 115200 bps

Switch#
```

5-17 show ip telnet server

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

show ip telnet server

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show ip telnet server

Server State: Enabled

Switch#
```

5-18 show ip http server

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

show ip http server

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show ip http server

ip http server state :  Enabled
Switch#
```

5-19 show ip http secure-server

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

show ip http secure-server

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show ip http secure-server

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

5-20 show password-recovery

This command is used to display the password recovery configuration.

show password-recovery

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the password recovery configuration.

Example

This example shows how to display the password recovery configuration.

```
Switch#show password-recovery

 Running Configuration  :Enabled
 NV-RAM Configuration   :Enabled

Switch#
```

5-21 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

This example shows how to display all session information.

```
Switch#show users

ID   Type          User-Name           Privilege    Login-Time     IP address
------------------------------------------------------------------------------
0    * console     admin               15           12M5S
1    telnet        monitoruser         2            3DT2H20M15S     172.171.160.100
10   SSH           123                 15           1M45S           172.171.160.100

Total Entries: 3

Switch#
```

5-22 telnet

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

telnet {*IP-ADDRESS* **|** *IPV6-ADDRESS* **|** *DOMAIN-NAME***} [***TCP-PORT***]**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the host.
IPV6-ADDRESS	Specifies the IPv6 address of the host.
DOMAIN-NAME	Specifies the Telnet destination host name.
TCP-PORT	(Optional) 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

None.

Command Mode

User/Privileged 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.

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 DGS-1520-28MP management interface which allows a user to login.

```
Switch#telnet 10.90.90.91

                  DGS-1520-28 Gigabit Ethernet Smart Managed Switch

                              Command Line Interface
                             Firmware: Build 1.01.004
           Copyright(C) 2022 D-Link Corporation. All rights reserved.

User Access Verification

Username:
```

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 23

 ERROR: Could not open a connection to host on server port 23.
Switch#telnet 10.90.90.91 3500

                      DGS-3630-28TC Gigabit Ethernet Switch

                              Command Line Interface
                             Firmware: Build 2.20.B007
           Copyright(C) 2018 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

5-23 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 **terminal length default** command will set the default value but it does not affect the current session. The newly created, saved session terminal length will use the default value. Use the **no** form of this command to revert to the default setting.

terminal length *NUMBER*

no terminal length

terminal length default *NUMBER*

no terminal length default

Parameters

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

Default

By default, this value is 24.

Command Mode

Use the User/Privileged 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, 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#
```

5-24 terminal speed

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

terminal speed *BPS*

no terminal speed

Parameters

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

Default

By default, this value is 115200.

Command Mode

Global Configuration Mode.

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)#
```

5-25 session-timeout

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

session-timeout *MINUTES*

no session-timeout

Parameters

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

Default

By default, this value is 3 minutes.

Command Mode

Line Configuration Mode.

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)#
```

5-26 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 does not affect any current sessions. Use the **no** form of this command to revert to the default setting.

terminal width *NUMBER*

no terminal width

terminal width default *NUMBER*

no terminal width default

Parameters

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

Default

By default, this value is 80 characters.

Command Mode

Use the User/Privileged 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#terminal width 120
Switch#
```

5-27 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 | 15]** *PASSWORD***]**

no username [*NAME***]**

Parameters

NAME	Specifies the user name with a maximum of 32 characters.
privilege *LEVEL*	(Optional) Specifies the privilege level for each user. The privilege level must be between 1 and 15. If this parameter is not specified, the privilege level is 1.
nopassword	(Optional) Specifies that there will be no password associated with this account.
password	(Optional) Specifies the password for the user.
0	(Optional) 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	(Optional) 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.
15	(Optional) Specifies the password in the encrypted form based on MD5. The password length is fixed at 31 bytes. It is case-sensitive. The password is encrypted. If the password syntax is not specified, the syntax is plain text.
PASSWORD	(Optional) Specifies the password string based on the type.

Default

By default, the user name is *admin*, password is *admin*, and the privilege level is 15.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command creates user accounts with different access levels. When the user logs in 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 logs in 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, 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)#
```

5-28 password

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

password [0 | 7 | 15] *PASSWORD*

no password

Parameters

0	(Optional) 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	(Optional) 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.
15	(Optional) Specifies the password in the encrypted form based on MD5. The password length is fixed at 31 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)#
```

5-29 clear line

This command is used to disconnect a connection session.

clear line *LINE-ID*

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

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

This command can only disconnect SSH and Telnet sessions.

Example

This example shows how to disconnect the line session 1.

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

5-30 banner exec

This command is used to configure the banner message to be displayed when an EXEC process is initiated. Use the **no** form of this command to delete the existing EXEC banner.

banner exec *cMESSAGEc*

no banner exec

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure a customized banner to be displayed before the EXEC mode prompt.

The customized banner allows using specific tokens in the form of $ in the message text to display the current configuration or information in the System.

- **$(hostname)** - The string that is used to define the prompt message.
- **$(line)** - Display the line ID (connection session ID).

Example

This example shows how to configure a EXEC banner. The token sign ($) is replaced by the corresponding configuration.

```
Switch(config)#banner exec #
Enter TEXT message.  End with the character '#'.
Session established on $(hostname)#
Switch(config)#
```

5-31 exec-banner

This command is used to display the EXEC banner on the specified line or lines. Use the **no** form of this command to revert to the default setting.

exec-banner

no exec-banner

Parameters

None.

Default

By default, this is enabled on all lines.

Command Mode

Line Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command determines whether the Switch displays the EXEC banner when an EXEC session is created.

Example

This example shows how to configure that the EXEC banner is not displayed on SSH line.

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-line)#no exec-banner
Switch(config-line)#
```

5-32 outgoing-session-timeout

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

outgoing-session-timeout *MINUTES*

no outgoing-session-timeout

Parameters

MINUTES	Specifies the timeout length in minutes. 0 represents never timeout. The value is from 0 to 1439.

Default

By default, this value is 0.

Command Mode

Line Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the outgoing session timeout value used to timeout outgoing Telnet connections through the CLI of the Switch to another device.

When the timeout occurs through a virtual line connection (Telnet/SSH connection to the Switch), the session will be returned to the Privileged EXEC Mode prompt.

When the timeout occurs through the physical line connection (Console connection to the Switch), the session will be logged out and the line connection will be returned to the idle state.

The outgoing session timeout function has a higher priority than the session timeout function (connection to the Switch) configured using the session-timeout command. This means that the local session cannot be closed if the outgoing session is still alive.

Example

This example shows how to configure the outgoing session timeout value for SSH line.

```
Switch#configure terminal
Switch(config)#line ssh
Switch(config-line)#outgoing-session-timeout 5
Switch(config-line)#
```

5-33 terminal monitor

The command is used to enable debugging and system log messages for current Telnet/SSH sessions. Use the **no** form of this command to disable this function.

terminal monitor

terminal no monitor

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable or disable debugging and system log messages for current Telnet/SSH sessions.

Example

This example shows how to enable debugging and system log messages for current Telnet/SSH sessions.

```
Switch#terminal monitor
Switch#
```

6. ARP Spoofing Prevention Commands

6-1 ip arp spoofing-prevention

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

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

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

Parameters

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

Default

By default, no entries exist.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

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 does not match the configured gateway IP address.

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

Example

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

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

6-2 ip arp spoofing-prevention logging enable

This command is used to enable logging the attack information when the IP address of the attack matches the gateway. Use the **no** form of this command to disable this function.

ip arp spoofing-prevention logging enable

no ip arp spoofing-prevention logging 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 logging the attack information when the IP address of the attack matches the gateway.

Example

This example shows how to enable logging the attack information when the IP address of the attack matches the gateway.

```
Switch#configure terminal
Switch(config)#ip arp spoofing-prevention logging enable
Switch(config)#
```

6-3 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/Privileged EXEC 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 eth1/0/10

Total Entries: 1

Switch#
```

Display Parameters

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

7. Asymmetric VLAN Commands

7-1 asymmetric-vlan

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

asymmetric-vlan

no asymmetric-vlan

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 asymmetric VLAN function.

Example

This example shows how to enable asymmetric VLAN.

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

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

8-1 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** form of this command to remove an accounting method list.

aaa accounting commands *LEVEL* **{default |** *LIST-NAME***} {start-stop** *METHOD1* **[***METHOD2***...] | none}**

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.
start-stop	Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server.
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 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 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+
Switch(config)#
```

8-2 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 this command to disable the accounting EXEC.

aaa accounting exec {default | *LIST-NAME***} {start-stop** *METHOD1* **[***METHOD2***...] | none}**

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.
start-stop	Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server.
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
Switch(config)#
```

8-3 aaa accounting network

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

aaa accounting network default {start-stop *METHOD1* **[***METHOD2***...] | none}**

no aaa accounting network default

Parameters

network	Specifies to perform accounting of network related service requests.
default	Specifies to configure the default method list for network accounting.
start-stop	Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server.
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 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
Switch(config)#
```

8-4 aaa accounting system

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

aaa accounting system default {start-stop *METHOD1* **[***METHOD2***...] | none}**

no aaa accounting system default

Parameters

system	Specifies to perform accounting for system-level events.
default	Specifies to configure the default method list for system accounting.
start-stop	Specifies to send accounting messages when a process starts and ends. Users are allowed to access the network, whether or not the start accounting message was received by the accounting server.
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 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
Switch(config)#
```

8-5 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** form of this 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
Switch(config)#
```

8-6 aaa authentication dot1x

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

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

no aaa authentication dot1x default

Parameters

METHOD1 **[***METHOD2***...]**	Specifies the list of methods that the authentication algorithm tries in the given sequence. Enter at least one method or enter up to four methods. The following are keywords that can be used to specify a method. **local** - Specifies to use the local database for authentication. **group radius** - Specifies to use the servers defined by the RADIUS server host command. **group** *GROUP-NAME* - Specifies to use the server groups defined by the AAA group server. **none** - Normally, the method is listed as the last method. The user will pass 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
Switch(config)#
```

8-7 aaa authentication igmp-auth

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

aaa authentication igmp-auth default group radius

no aaa authentication igmp-auth default

Parameters

None.

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 IGMP authentication.

Example

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

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

8-8 aaa authentication login

This command is used to configure the method list used for login authentication Use the **no** form of this 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, 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
Switch(config)#
```

8-9 aaa authentication mac-auth

This command is used to configure the default method list used for MAC authentication. Use the **no** form of this 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
Switch(config)#
```

8-10 aaa authentication web-auth

This command is used to configure the default method list used for Web authentication. Use the **no** form of this 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
Switch(config)#
```

8-11 aaa group server radius

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

aaa group server radius *GROUP-NAME*

no aaa group server radius *GROUP-NAME*

Parameters

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

Default

There is no AAA group server.

Command Mode

Global Configuration Mode.

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 the **aaa authentication** and **aaa accounting** commands. Also use this command to enter the RADIUS Group Server Configuration Mode. Use the **server** command to associate the RADIUS server hosts with the RADIUS server group.

Example

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

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

8-12 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 this 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 and 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** commands.

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+)#
```

8-13 aaa new-model

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

aaa new-model

no aaa new-model

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

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
Switch(config)#
```

8-14 aaa server radius dynamic-author

This command is used to configure the Switch as an AAA server to facilitate interaction with an external policy server. Use the **no** form of this command to disable this function.

aaa server radius dynamic-author

no aaa server radius dynamic-author

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Dynamic authorization allows an external policy server to dynamically send updated to a device. Use this command to configure the Switch as an AAA server and enter the Dynamic Authorization Local Server Configuration Mode.

Example

This example shows how to enter the Dynamic Authorization Local Server Configuration Mode.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#
```

8-15 accounting commands

This command is used to configure the method list used for command accounting via a specific line. Use the **no** form of this 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)#
```

8-16 accounting exec

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

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 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
Switch(config-line)#
```

8-17 clear aaa counters servers

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

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

Parameters

all	Specifies to clear server counter information related to all server hosts.
radius *IP-ADDRESS*	Specifies to clear server counter information related to a RADIUS IPv4 host.
radius *IPV6-ADDRESS*	Specifies to clear server counter information related to a RADIUS IPv6 host.
radius all	Specifies to clear server counter information related to all RADIUS hosts.
tacacs *IP-ADDRESS*	Specifies to clear server counter information related to a TACACS IPv4 host.
tacacs *IPV6-ADDRESS*	Specifies to clear server counter information related to a TACACS IPv6 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

Privileged 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#
```

8-18 client

This command is used to configure a RADIUS client from which the Switch can accept Change of Authorization (CoA) and disconnect requests. Use the **no** form of this command to remove the configuration.

client {*IP-ADDRESS* **|** *HOST-NAME***} server-key [0 | 7]** *STRING*

no client {*HOST-NAME* **|** *IP-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IP address of the RADIUS client.
HOST-NAME	Specifies the host name of the RADIUS client.
server-key	Specifies the RADIUS key to be shared between the Switch and the RADIUS client.
0	(Optional) Specifies the key in the clear text form. If neither 0 nor 7 are specified, this is the default option.
7	(Optional) Specifies the password in the encrypted form.
STRING	Specifies the shared key.

Default

By default, CoA and disconnect requests are dropped.

Command Mode

Dynamic Authorization Local Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

The Switch can be configured to allow an external policy server to dynamically send updates to the Switch. This functionality is facilitated by the CoA RADIUS extension. CoA introduces peer-to-peer capability to RADIUS, enabling the Switch to act as a server and the external policy server to act as a client.

Use this command to configure RADIUS clients for which the Switch can act as a RADIUS server.

Example

This example shows how to configure the Switch to accept request from a RADIUS client.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#client 10.0.0.1 server-key 12345
Switch(config-locsvr-da-radius)#
```

8-19 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 this 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)#
```

8-20 ip http accounting exec

This command is used to specify an AAA accounting method for HTTP server users. Use the **no** form of this 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)#
```

8-21 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. Use the **no** form of this command to revert to the default setting.

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.

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
Switch(config)#
```

8-22 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. Use the **no** form of this command to revert to the default setting.

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.

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
Switch(config)#
```

8-23 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. Use the **no** form of this command to revert to the default setting.

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.

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
Switch(config)#
```

8-24 ipv6 tacacs source-interface

This command is used to specify the interface whose IPv6 address will be used as the source IPv6 address for sending TACACS packets. Use the **no** form of this command to revert to the default setting.

ipv6 tacacs source-interface *INTERFACE-ID*

no ipv6 tacacs source-interface

Parameters

INTERFACE_ID	Specifies the interface whose IPv6 address will be used as the source IPv6 address for sending TACACS packets.

Default

The IPv6 address of the closest interface will be used.

Command Mode

Global Configuration Mode.

Server Group Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command can be used to specify the interface whose IPv6 address will be used as the source IPv6 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 IPv6 address will be used as the source IPv6 address, for sending TACACS packets.

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

8-25 login authentication

This command is used to configure the method list used for login authentication via a specific line. Use the **no** form of this command to revert 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)#
```

8-26 port

This command is used to configure the port that listens for RADIUS requests from RADIUS clients. Use the **no** form of this command to revert to the default setting.

port *PORT-NUMBER*

no port

Parameters

PORT-NUMBER	Specifies the port number.

Default

The default port number is 3799.

Command Mode

Dynamic Authorization Local Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the port that listens for RADIUS requests from RADIUS clients.

Example

This example shows how to configure the port number as 1650 that listens for RADIUS requests.

```
Switch#configure terminal
Switch(config)#aaa server radius dynamic-author
Switch(config-locsvr-da-radius)#port 1650
Switch(config-locsvr-da-radius)#
```

8-27 radius-server attribute 4

This command is used to specify the IP address for the RADIUS attribute 4 address. Use the **no** form of this command to delete the IP address.

radius-server attribute 4 *IP-ADDRESS*

no radius-server attribute 4 *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IP address for the RADIUS attribute 4 address.

Default

By default, the IP address is the IP address on the interface that connects the NAS to the RADIUS server.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Normally, when the **ip radius source-interface** command is configured, the specified IP address is used as the IP address in the IP headers of the RADIUS packets, and as the RADIUS attribute 4 address inside the RADIUS packets.

However, when the **radius-server attribute 4** command is configured, the specified IP address is used as the RADIUS attribute 4 address inside the RADIUS packets. There is no impact to the IP address in the IP headers of the RADIUS packets.

Example

This example shows how to configure the RADIUS attribute 4 address as 10.0.0.21.

```
Switch#configure terminal
Switch(config)#radius-server attribute 4 10.0.0.21
Switch(config)#
```

8-28 radius-server attribute 55 include-in-acct-req

This command is used to send the RADIUS attribute 55 (Event-Timestamp) in accounting packets. Use the **no** form of this command to revert to the default setting.

radius-server attribute 55 include-in-acct-req

no radius-server attribute 55 include-in-acct-req

Parameters

None.

Default

By default, the RADIUS attribute 55 is not sent.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to send the RADIUS attribute 55 in accounting packets.

Example

This example shows how to enable the sending of the RADIUS attribute 55.

```
Switch#configure terminal
Switch(config)#radius-server attribute 55 include-in-acct-req
Switch(config)#
```

8-29 radius-server deadtime

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

radius-server deadtime *MINUTES*

no radius-server deadtime

Parameters

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

Default

By default, this value is 0.

Command Mode

Global Configuration Mode.

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
Switch(config)#
```

8-30 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*	(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*	(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*	(Optional) Specifies the server time-out value. The range of timeout is between 1 and 255 seconds. If this parameter is 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 this parameter is not specified, the default value is 2.
Key 0 *KEY-STRING*	Specifies the unencrypted (cleartext) shared key. This key can be from 1 to 254 characters long.

Key 7 *KEY-STRING*	Specifies the encrypted shared key. This key can be from 24 to 344 characters long.

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
Switch(config)#
```

8-31 server (RADIUS)

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

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

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

Parameters

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

Default

By default, no server is configured.

Command Mode

RADIUS Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

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

8-32 server (TACACS+)

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

Command Mode

TACACS+ Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this 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** commands. 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+)#
```

8-33 show aaa

This command is used to display the AAA global state.

show aaa

Parameters

None.

Default

None.

Command Mode

Privileged EXEC 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#
```

8-34 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* | *IPV6-ADDRESS***} [port** *PORT-NUMBER***] [timeout** *SECONDS***] key [0 | 7]** *KEY-STRING*

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

Parameters

IP-ADDRESS	Specifies the IPv4 address of the TACACS+ server.
IPV6-ADDRESS	Specifies the IPv6 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)#
```

8-35 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

User/Privileged EXEC 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: 10.90.90.211: Auth-Port 1812, Acct-Port 1813
 State is Up
                          Auth.       Acct.
 Round Trip Time:         2           0
 Access Requests:         2           NA
 Access Accepts:          1           NA
 Access Rejects:          0           NA
 Access Challenges:       1           NA
 Acct Request:            NA          0
 Acct Response:           NA          0
 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


Switch#
```

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.

8-36 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

User/Privileged EXEC 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: 10.90.90.5/49, State is Up
 Socket Opens: 0
 Socket Closes: 0
 Total Packets Sent: 0
 Total Packets Recv: 0
 Reference Count: 0


Switch#
```

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.

9. Basic IPv4 Commands

9-1 arp

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

arp *IP-ADDRESS HARDWARE-ADDRESS*

no arp *IP-ADDRESS HARDWARE-ADDRESS*

Parameters

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

Default

No static entries are installed in the ARP cache.

Command Mode

Global Configuration Mode.

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
Switch(config)#
```

9-2 arp timeout

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

arp timeout *MINUTES*

no arp timeout

Parameters

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

Default

The default value is 240 minutes.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Used to set the ARP aging time for the ARP table.

Example

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

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

9-3 clear arp-cache

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

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

Parameters

all	Specifies to clear the dynamic ARP cache entries associated with all interfaces.
INTERFACE-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#
```

9-4 ip address

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

ip address {*IP-ADDRESS SUBNET-MASK* **[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.

The default IP address of the MGMT port is 192.168.0.1/24.

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.

The **dhcp** parameter is not supported on the MGMT port.

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)#
```

9-5 ip default-gateway

This command is used to configure the default gateway IP address of the management port. Use **no** command to remove the default gateway IP address.

ip default-gateway *IP-ADDRESS*

no ip default-gateway *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IPv4 address of the default gateway here.

Default

By default, the default gateway IP address is 0.0.0.0.

Command Mode

MGMT Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

IP packets destined to other IP subnets are sent to the default gateway. This command can only be used in the MGMT Interface Configuration Mode.

Example

This example shows how to configure the default gateway IP address of the MGMT interface to 192.168.0.254.

```
Switch#configure terminal
Switch(config)#interface mgmt0
Switch(config-if)#ip default-gateway 192.168.0.254
Switch(config-if)#
```

9-6 ip proxy-arp

This command is used to enable the proxy ARP option for an interface. Use the **no** form of this 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)#
```

9-7 ip local-proxy-arp

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

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)#
```

9-8 ip mtu

This command is used to set the MTU value. Use the **no** form of this command 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)#
```

9-9 show arp

This command is used to display the ARP cache.

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

Parameters

ARP-TYPE	(Optional) Specifies the ARP type. **dynamic** – Specifies to display only dynamic ARP entries. **static** –Specifies to display only static ARP entries.
IP-ADDRESS [*MASK*]	(Optional) Specifies to display a specific entry or entries that belong to a specific network.
INTERFACE-ID	(Optional) Specifies to display ARP entries that are associated with a specific network.
HARDWARE-ADDRESS	(Optional) Specifies to display ARP entries whose hardware address equal to this address

Default

None.

Command Mode

User/Privileged EXEC 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#
```

9-10 show arp timeout

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

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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#
```

9-11 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/Privileged EXEC 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. **(DGS-1520-28 and DGS-1520-52 Only)**

```
Switch#show ip interface brief


Interface    IP Address      Link Status
----------  ---------------  -----------
vlan1       10.90.90.90      up
mgmt_ipif   192.168.0.1      down

Total Entries: 2

Switch#
```

This example shows how to display the brief information of the IP interface. **(DGS-1520-28MP and DGS-1520-52MP Only)**

```
Switch#show ip interface brief


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

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface vlan 1

Interface vlan1 is enabled, Link status is up
  IP address is 10.90.90.90/8 (Manual)
  ARP timeout is 240 minutes.
  IP MTU is 1500 bytes
  Helper Address is not set
  Proxy ARP is disabled
  IP Local Proxy ARP is disabled
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface loopback 1

Interface loopback1 is enabled
  IP address is 192.168.1.1/24 (Manual)

Total Entries: 1

Switch#
```

10. Basic IPv6 Commands

10-1 clear ipv6 neighbors

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

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

Parameters

all	Specifies to clear the dynamic neighbor cache entries associated with all interfaces.
interface *INTERFACE-ID*	Specifies to clear dynamic neighbor cache entries associated with the specified interface 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#clear ipv6 neighbors interface vlan 1
Switch#
```

10-2 ipv6 address

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

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

no ipv6 address {*IPV6-ADDRESSIPREFIX-LENGTH* **|** *PREFIX-NAME SUB-BITSIPREFIX-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 12 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.

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
```

10-3 ipv6 address eui-64

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

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

no ipv6 address *IPV6-PREFIX/PREFIX-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

Use this command to configure an IPv6 address on the interface using the EUI-64 interface ID.

Example

This example shows how to add an IPv6 address incidence.

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

10-4 ipv6 address dhcp

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

ipv6 address dhcp [rapid-commit]

no ipv6 address dhcp

Parameters

rapid-commit	(Optional) Specifies to use a two-message exchange instead of the standard four-message exchange between the Requesting Router (RR) and the Delegating Router (DR) to obtain the network configuration settings from the DHCP Server.

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 interface to obtain IPv6 network configuration settings from a DHCPv6 server.

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

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

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

Example

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

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

10-5 ipv6 address autoconfig

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

ipv6 address autoconfig [default]

no ipv6 address autoconfig

Parameters

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

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only available for the VLAN IPv6 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** parameter is specified, it will accord the received router advertisement to insert a default route to the IPv6 routing table. The type of this default route is SLAAC. It has higher route preference than the dynamic default route which is learnt from RIPng and OSPFv3.

When the auto-configuration function is already enabled, the **no** command must be issued before the **ipv6 address autoconfig default** command can be issued and vice versa.

Example

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

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

10-6 ipv6 enable

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

ipv6 enable

no ipv6 enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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)#
```

10-7 ipv6 hop-limit

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

ipv6 hop-limit *VALUE*

no ipv6 hop-limit

Parameters

VALUE	Specifies the IPv6 hop limit range. Using the value 0 means to use the default value to send packets. The valid range is 0 to 255.

Default

By default, this value is 64.

Command Mode

Interface 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)#
```

10-8 ipv6 mtu

This command is used to configure the MTU value for IPv6. Use the **no** form of this command 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)#
```

10-9 ipv6 nd managed-config-flag

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

ipv6 nd managed-config-flag

no ipv6 nd managed-config-flag

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Example

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

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

10-10 ipv6 nd other-config-flag

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

ipv6 nd other-config-flag

no ipv6 nd other-config-flag

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Example

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

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

10-11 ipv6 nd prefix

This command is used to configure an IPv6 prefix to be advertised in RA messages. Use the **no** form of this 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 this parameter is 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 this parameter is not specified, the default preferred lifetime value is 604800 seconds (7 days).
off-link	(Optional) Specifies to turn off the on-link flag. If this parameter is not specified, the default off-link flag is ON.
no-autoconfig	(Optional) Specifies to turn off the auto-configure flag. If this parameter is 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** parameters are not specified.
  - The prefix is inserted in the routing table. L bit = 1, A bit = 1.
- Combination 2: The **no-autoconfig** parameter is specified.
  - The prefix is inserted in the routing table. L bit = 1, A bit = 0.
- Combination 3: The **off-link** parameter 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, 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, 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)#
```

10-12 ipv6 nd ra interval

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

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

no ipv6 nd ra interval

Parameters

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

Default

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)#
```

10-13 ipv6 nd ra lifetime

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

ipv6 nd ra lifetime *SECONDS*

no ipv6 nd ra lifetime

Parameters

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

Default

By default, this value is 1800 seconds.

Command Mode

Interface Configuration Mode.

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)#
```

10-14 ipv6 nd suppress-ra

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

ipv6 nd suppress-ra

no ipv6 nd suppress-ra

Parameters

None.

Default

RA is disabled on the VLAN interface.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

10-15 ipv6 nd reachable-time

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

ipv6 nd reachable-time *MILLI-SECONDS*

no ipv6 nd reachable-time

Parameters

MILLI-SECONDS	Specifies the IPv6 router advertisement reachable time range in milliseconds. 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 30 seconds on the interface and advertise 0 (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)#
```

10-16 ipv6 nd ns-interval

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

ipv6 nd ns-interval *MILLI-SECONDS*

no ipv6 nd ns-interval

Parameters

MILLI-SECONDS	Specifies the amount of time between retransmissions of NS message 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)#
```

10-17 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** *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 *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 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 interface vlan 1 00-01-80-11-22-99
Switch(config)#
```

10-18 ipv6 optimistic dad

This command is used to enable the IPv6 Optimistic Duplicate Address Detection (DAD) state. Use the **no** form of this command to disable this function.

ipv6 optimistic dad

no ipv6 optimistic dad

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the IPv6 Optimistic DAD state.

Example

This example shows how to enable the IPv6 Optimistic DAD state.

```
Switch#configure terminal
Switch(config)#ipv6 optimistic dad
Switch(config)#
```

10-19 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 12 characters.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

10-20 show ipv6 interface

This command is used to display IPv6 interface information.

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IPv6 interface related configurations.

Example

This example shows how to display IPv6 interface information.

```
Switch#show ipv6 interface vlan2

vlan2 is up, Link status is down
  IPv6 is enabled,
  link-local address:
      FE80::201:1FF:FE02:305
  Global unicast address:
      200::2/64 (DHCPv6 PD)
  IPv6 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

Total Entries: 1

Switch#
```

This example shows how to display brief IPv6 interface information.

```
Switch#show ipv6 interface brief

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

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

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

Total Entries: 3

Switch#
```

10-21 show ipv6 neighbors

This command is used to display IPv6 neighbor information.

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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. **DELAY** - The neighbor is no longer known to be reachable and traffic has recently been sent to the neighbor. Instead of probing the neighbor immediately, delay the sending of probes for a short while in order to give upper-layer protocols a chance to provide reachability confirmation.

10-22 show ipv6 optimistic dad

This command is used to display IPv6 Optimistic DAD state.

show ipv6 optimistic dad

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IPv6 Optimistic DAD state

Example

This example shows how to display IPv6 Optimistic DAD state.

```
Switch#show ipv6 optimistic dad

IPv6 Optimistic DAD State: Enabled

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 revert 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 blocks 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

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

Use this command to enable and configure the BPDU protection operational mode.

Example

This example shows how to enable the BPDU Protection function with block mode on port 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*	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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        -
eth1/0/4           Disabled     Shutdown     Normal
eth1/0/5           Disabled     Shutdown     Normal
eth1/0/6           Disabled     Shutdown     Normal
eth1/0/7           Disabled     Shutdown     Normal
eth1/0/8           Disabled     Shutdown     Normal
eth1/0/9           Disabled     Shutdown     Normal
eth1/0/10          Disabled     Shutdown     Normal
eth1/0/11          Disabled     Shutdown     Normal
eth1/0/12          Disabled     Shutdown     Normal
eth1/0/13          Disabled     Shutdown     Normal
eth1/0/14          Disabled     Shutdown     Normal
eth1/0/15          Disabled     Shutdown     Normal
eth1/0/16          Disabled     Shutdown     Normal
eth1/0/17          Disabled     Shutdown     Normal
eth1/0/18          Disabled     Shutdown     Normal
eth1/0/19          Disabled     Shutdown     Normal
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the BPDU protection status of port 1.

```
Switch#show spanning-tree bpdu-protection interface eth1/0/1

Interface          State        Mode         Status
--------------     --------     --------     ------------
eth1/0/1           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.

11-4 snmp-server enable traps stp-bpdu-protection

This command is used to enable the sending of SNMP notifications for BPDU protection. Use the **no** form of this command to disable the sending of SNMP notifications for BPDU protection.

snmp-server enable traps stp-bpdu-protection

no snmp-server enable traps stp-bpdu-protection

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

None.

Example

This example shows how to enable the sending of SNMP notifications for BPDU protection.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps stp-bpdu-protection
Switch(config)#
```

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

Default

None.

Command Mode

EXEC Mode.

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 eth1/0/1
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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

EXEC Mode.

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)
--------- ---------- ------------- ------------------------- -----------------
eth1/0/1  1000BASE-T Link Down     Shutdown                  2
eth1/0/2  1000BASE-T Link Down     -                         -
eth1/0/3  1000BASE-T Link Down     -                         -
eth1/0/4  1000BASE-T Link Down     -                         -
eth1/0/5  1000BASE-T Link Down     -                         -
eth1/0/6  1000BASE-T Link Down     -                         -
eth1/0/7  1000BASE-T Link Down     -                         -
eth1/0/8  1000BASE-T Link Down     -                         -
eth1/0/9  1000BASE-T Link Down     -                         -
eth1/0/10 1000BASE-T Link Down     -                         -
eth1/0/11 1000BASE-T Link Down     -                         -
eth1/0/12 1000BASE-T Link Down     -                         -
eth1/0/13 1000BASE-T Link Down     -                         -
eth1/0/14 1000BASE-T Link Down     -                         -
eth1/0/15 1000BASE-T Link Down     -                         -
eth1/0/16 1000BASE-T Link Down     -                         -
eth1/0/17 1000BASE-T Link Down     -                         -
eth1/0/18 1000BASE-T Link Down     -                         -
eth1/0/19 1000BASE-T Link Down     -                         -
eth1/0/20 1000BASE-T Link Down     -                         -
eth1/0/21 1000BASE-T Link Down     -                         -
eth1/0/22 1000BASE-T Link Down     -                         -
eth1/0/23 1000BASE-T Link Down     -                         -
eth1/0/24 1000BASE-T Link Down     -                         -
```

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

Default

None.

Command Mode

EXEC Mode.

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 eth1/0/1
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: 12.

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. CPU Access Control List (ACL) Commands

14-1 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** form of this 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)#
```

14-2 match access-group

This command is used to associate an access list to the software ACL filter map. Use the **no** form of this 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 0.0.255.255
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)#
```

14-3 match interface

This command is used to configure matching ingress interface(s). Use the **no** form of this 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 interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
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 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 activate the software ACL filter map called "cpu_filter" on port 1.

```
Switch#configure terminal
Switch(config)#ip access-list cpu-acl
Switch(config-ip-acl)#permit 10.20.0.0 0.0.255.255
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)#
```

14-4 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

User/Privileged EXEC 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):cpu-acl
      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.

15. CPU Port Statistics Commands

15-1 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	(Optional) Specifies to display statistic counters of Layer 3 unicast routing and Layer 3 application control packets.
multicast	(Optional) Specifies to display statistic counters of Layer 3 multicast routing control packets.
protocol *NAME*	(Optional) Specifies the name of protocol.

Default

None.

Command Mode

Privileged EXEC 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
--------------------------------- ---------- ----------- -----------
802.1X                            0          0           0
ARP                               0          2           0
CTP                               0          0           0
DHCP                              0          0           0
DHCPv6                            0          0           0
DNS                               0          0           0
DVMRP                             0          0           0
ERPS                              0          0           0
GVRP                              0          0           0
ICMP                              0          0           0
ICMPv6                            0          0           0
IGMP                              0          0           0
LACP                              0          0           0
LLDP                              0          0           0
MLD                               0          0           0
NDP                               0          0           0
OSPFv2                            0          0           0
OSPFv3                            0          0           0
PIM-IPv4                          0          0           0
PIM-IPv6                          0          0           0
Reserved-IPv4-IPMC                0          0           0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

15-2 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#
```

16. Debug Commands

16-1 debug enable

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

debug enable

no debug enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to enable or disable the debug message output option.

Example

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

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

16-2 debug output

This command is used to specify the output for the debug messages of individual modules. Use the **no** form of this command to disable the function.

debug output {module *MODULE-LIST* **| all} {buffer | console | monitor}**

no debug output {module *MODULE-LIST* **| all}**

Parameters

MODULE-LIST	Specifies the module list to output the debug messages. Enclose module list items with double quotation marks and leave a space between module list items.
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.

monitor	Specifies to output the debug messages to terminal such as Telnet or SSH.

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 **debug show 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 output the debug messages of MSTP to the local console.

```
Switch#debug output module "MSTP" console
Switch#
```

This example shows how to configure all the module's debug messages to output to the debug buffer.

```
Switch#debug output all buffer
Switch#
```

16-3 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 or disable the Switch to reboot when a fatal error occurs.

Example

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

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

16-4 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:** *IILOCATIONIDESTINATION-URL*

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.
DESTINATION-URL	Specifies the destination URL.
LOCATION	Specifies the IPv4 or IPv6 address of the TFTP server.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

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

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

Switch#
```

16-5 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
Clear debug-buffer? (y/n) [n]  y
Switch#
```

16-6 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#
```

16-7 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.

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. If no parameter is specified, the content in the buffer will be displayed.

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#
```

16-8 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
----------------      --------  ---------------------------------------
MSTP                  buffer    No
OSPFV2                buffer    No
VRRP                  buffer    No
RIPNG                 buffer    No

Switch#
```

16-9 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 : 2022/11/01 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 : 2022/11/01 15:00:00
====================== SOFTWARE FATAL ERROR ======================
CLI_UTL_AllocateMemory Fail!

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

Total Log : 2

Switch#
```

16-10 debug show tech-support

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

debug show tech-support [unit *UNIT-ID***]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the unit ID in the stacking system.

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. If no parameter is specified, all units are displayed.

Example

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

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#                DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
#                         Technical Support Information
#
#                           Firmware: Build 1.01.004
#    Copyright(C) 2022  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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

[SYS 2019-1-1 00:03:10]

Boot Time           : 1 Jan 2019  00:00:00
RTC Time            : 2019/01/01 00:03:10
Boot PROM Version   : Build 1.00.011
Firmware Version    : Build 1.01.004
Hardware Version    : A1
Serial number       : DGS1520-28MPA
MAC Address         : 80-26-89-15-28-00
MAC Address Number  : 29

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

16-11 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 -   7 %         One minute -   6 %         Five minutes -  17 %

Process Name         5Sec     1Min     5Min
-----------------   ------   ------   ------
tIdleTask0           93 %     94 %     83 %
bcmL2X.0              1 %      1 %      1 %
bcmCNTR.0             1 %      1 %      1 %
cpuprotect            0 %      0 %      0 %
bcmLINK.0             0 %      0 %      0 %
hisr1                 0 %      0 %      0 %
socdmadesc.0          0 %      0 %      0 %
poe_task              0 %      0 %      0 %
MAUMIB_TASK           0 %      0 %      0 %
FWD-ETH               0 %      0 %      0 %
IP-Msg                0 %      0 %      0 %
bcmRX                 0 %      0 %      0 %
web                   0 %      0 %      0 %
CNT_TASK              0 %      0 %      0 %
bcmMEM_SCAN.0         0 %      0 %      0 %
CLI                   0 %      0 %      0 %
OS_TIMER              0 %      0 %      0 %
8021xCtrl             0 %      0 %      0 %
HISTORCNT_TASK        0 %      0 %      0 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

17. DHCP Auto-Configuration Commands

17-1 autoconfig enable

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

autoconfig enable

no autoconfig enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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 enable auto-configuration.

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

 WARNING:Autoconfig enabled now, but won't take effect until reboot.
Switch(config)#
```

17-2 show autoconfig

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

show autoconfig

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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: Enabled

Switch#
```

18. DHCP Auto-Image Commands

18-1 autoimage enable

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

autoimage enable

no autoimage enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

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

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

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

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

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

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

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

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

Example

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

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

18-2 autoimage timeout

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

autoimage timeout *SECONDS*

Parameters

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

Default

By default, the value is 50 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

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

18-3 show autoimage

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

show autoimage

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show autoimage

Autoimage State: Disabled
Timeout        : 60

Switch#
```

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 to the default setting.

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 *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.

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 to the default setting.

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 class (DHCP Relay)

This command is used to enter the DHCP Pool Class Configuration Mode and associate a range of IP addresses with the DHCP class. Use the **no** form of this command to remove the association.

class *NAME*

no class *NAME*

Parameters

NAME	Specifies the DHCP class name. This name can be up to 32 characters long.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12

Usage Guideline

This command is used to associate a DHCP relay pool with a DHCP pool class. Use the **relay target** command to define the list of relay target addresses for DHCP packet forwarding. If the DHCP client request matches a relay pool, which is configured with classes, the client must match a class configured in the pool in order to be relayed. If no DHCP class is configured, 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 to configure a DHCP class, “Service-A”, defined with DHCP Option 60 matching pattern 0x112233 and 0x102030, classified to the relay pool, "pool1", and is associated with relay target "10.2.1.2".

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

20-2 ip dhcp class (DHCP Relay)

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

ip dhcp class *NAME*

no ip dhcp class *NAME*

Parameters

NAME	Specifies the DHCP class name. 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 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)#
```

20-3 ip dhcp pool (DHCP Relay)

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

ip dhcp pool *NAME*

no ip dhcp pool *NAME*

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

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.

Example

This example shows how to create a DHCP relay pool, called pool1. In the relay pool, the subnet 172.19.18.0/255.255.255.0 is specified as the source subnet. 10.2.1.1 is specified as the relay destination address.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#relay source 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#relay destination 10.2.1.1
Switch(config-dhcp-pool)#
```

20-4 ip dhcp relay information check

This command is used to enable the DHCP relay agent to validate and remove the relay agent information option in the received DHCP reply packet. Use the **no** form of this command to globally disable the check for Option 82.

ip dhcp relay information check

no ip dhcp relay information check

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

The **ip dhcp relay information check** command and the **ip dhcp relay information check-reply** command together determine whether the check function of Option 82 is effective for an interface. If the **ip dhcp relay information check-reply** command is not configured for an interface, the global setting takes effect. If the **ip dhcp relay information check-reply** command is configured for an interface, the interface setting takes effect.

When the check for Option 82 of the reply packet is enabled, the device will check the validity of the Option 82 field in DHCP reply packets it receives from the DHCP server. If the Option 82 field in the received packet is not present or the option is not the original option inserted by the agent (by checking the remote ID sub-option, the relay agent drops the packet. Otherwise, the relay agent removes the Option 82 field and forwards the packet.

If the check is disabled, the packet will be directly forwarded.

Example

This example shows how to enable the global DHCP relay agent check.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information check
Switch(config)#
```

20-5 ip dhcp relay information check-reply

This command is used to configure the DHCP relay agent to validate the relay agent information option in the received DHCP reply packet. Use the **no** form of this command to remove the configuration for the interface.

ip dhcp relay information check-reply [none]

no ip dhcp relay information check-reply [none]

Parameters

none	(Optional) Specifies to disable check for Option 82 of the reply packet.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

The **ip dhcp relay information check** command and the **ip dhcp relay information check-reply** command together determine whether the check function of Option 82 is effective for an interface. If the **ip dhcp relay information check-reply** command is not configured for an interface, the global setting takes effect. If the **ip dhcp relay information check-reply** command is configured for an interface, the interface setting takes effect.

When the check for Option 82 of the reply packet is enabled, the device will check the validity of the Option 82 field in DHCP reply packets it receives from the DHCP server. If the Option 82 field in the received packet is not present or the option is not the original option inserted by the agent (by checking the remote ID sub-option), the relay agent drops the packet. Otherwise, the relay agent removes the Option 82 field and forwards the packet.

If the check is disabled, the packet will be directly forwarded.

Example

This example shows how to disable the global DHCP relay agent check but 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
Switch(config-if)#
```

20-6 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** form of this 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

This command takes effect when the **service dhcp** command is enabled.

When DHCP Option 82 is enabled, the DHCP packet received from the client will be inserted with an Option 82 field before being relayed to the server. The DHCP Option 82 contains two sub-options respectively the circuit ID sub-option and remote ID sub-option.

Administrators can use the **ip dhcp relay information option format remote-id** command to specify a user-defined string for the remote ID sub-option.

Example

This example shows how to enable the insertion of Option 82 during the relay of DHCP request packets.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option
Switch(config)#
```

20-7 ip dhcp relay information option-insert

This command is used to configure the insertion of Option 82 for an interface during the relay of DHCP request packets. Use the **no** form of this 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 [none]

Parameters

none	(Optional) 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 **service dhcp** command 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)#
```

20-8 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 this command to revert to the default setting.

ip dhcp relay information policy {drop | keep | replace}

no ip dhcp relay information policy

Parameters

drop	Specifies to discard the packet that already has the relay option.
keep	Specifies that the DHCP requests packet that already has the relay option is left unchanged and directly relayed to the DHCP server.
replace	Specifies that the DHCP request packet that already has the relay option will be replaced by a new option.

Default

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

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

Use this command to configure the global policy for the insertion of Option 82 on packets that already have Option 82.

When this command is configured but not the **ip dhcp relay information policy-action** command in the Interface Configuration Mode, this configuration is applied to all interfaces.

Example

This example shows how to configure the relay agent option re-forwarding policy to keep.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information policy keep
Switch(config)#
```

20-9 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 this command to remove the configuration for the interface.

ip dhcp relay information policy-action {drop | keep | replace}

no ip dhcp relay information policy-action

Parameters

drop	Specifies to discard the packet that already has the relay option.
keep	Specifies that the DHCP request packet that already has the relay option is left unchanged and directly relayed to the DHCP server.
replace	Specifies that the DHCP request packet that already has the relay option will be replaced by a new option.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the **service dhcp** command is enabled.

Use this command to configure the policy for the insertion of Option 82 on packets that already have Option 82 for an interface.

Example

This example shows how to configure the relay agent option re-forwarding policy to keep and set the policy to drop for VLAN 100. The effective relay agent option re-forwarding policy for VLAN 100 is drop and for the remaining interfaces are set as keep.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information policy keep
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information policy-action drop
Switch(config-if)#
```

20-10 ip dhcp relay information option format remote-id

This command is used to configure the DHCP information remote ID sub-option. Use the **no** form of this command to configure the default remote ID sub-option.

ip dhcp relay information option format remote-id {default| string *STRING* **| vendor2 | vendor3 | expert-udf [{standalone_unit_format {0 | 1}}]}**

no ip dhcp relay information option format remote-id

Parameters

default — Specifies to use the Switch's system MAC address as the remote ID. The remote ID is formed in the following format:

a.	b.	c.	d.	e.
2	8	0	6	MAC Address
1 byte	1 byte	1 byte	1 byte	6 bytes

string *STRING* — Specifies to use a user-defined string as the remote ID. Space characters are allowed in the string. The remote ID option is formed in the following format:

a.	b.	c.	d.	e.
2	n+2	1	n	User Defined
1 byte	1 byte	1 byte	1 byte	Max. 32 bytes

vendor2 — Specifies to use the vendor 2. If configures, the remote ID option uses the original format:

a.	b.	c.
2	n	System Name
1 byte	1 byte	n byte

a. *Sub-option type:* The number 2 indicates that this is the remote ID.

b. *Length:* The length of the value.

c. *Value:* The character string. The system name of the Switch.

vendor3	Specifies to use the vendor 3. If configures, the remote ID option uses the original format: |---| | a. | b. | c. | |--------|--------|-------------------------------------| | 2 | n | User Defined | |--------|--------|-------------------------------------| | 1 byte | 1 byte | Max. 251 bytes | |---| **a.** *Sub-option type:* The number 2 indicates that this is the remote ID. **b.** *Length:* Total length of user-defined string. By default, Length is 0 and no value field. **c.** *Value:* Flexible user-defined string that configured through the **ip dhcp relay information option format-type remote-id vendor3 string** *STRING* command. The maximum length is 32.
expert-udf	Specifies to use expert-udf. If configures, the remote ID option uses the original format: |---| | a. | b. | c. | |---| | 2 | n | User Defined | |---| | 1 byte | 1 byte | Max. 251 bytes | |---| **a.** *Sub-option type:* The number 2 indicates that this is the remote ID. **b.** *Length:* Total length of user-defined string. By default, Length is 0 and no value field. **c.** *Value:* Flexible user-defined string that configured through the **ip dhcp relay information option format-type remote-id** and **ip dhcp relay information profile** commands. The maximum length is 251.
standalone_unit_format	Specifies the unit ID for the standalone unit. The default value is 0.

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

Use this command to select different vendor’s remote ID format or configures a user-defined string of ASCII characters to be the remote ID.

Example

This example shows how to use vendor2 as the remote ID.

```
Switch#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)#
```

20-11 ip dhcp relay information option format-type remote-id

This command is used to configure the DHCP information remote ID sub-option of vendor format string in the Interface Configuration Mode. Use the **no** form of this command to remove the remote ID sub-option of vendor format string.

ip dhcp relay information option format-type remote-id {vendor3 string *STRING* **| expert-udf** *NAME***}**

no ip dhcp relay information option format-type remote-id

Parameters

vendor3	Specifies the vendor 3 user-defined string. The maximum length of the string is 32.
STRING	Specifies the vendor-defined string.
expert-udf	Specifies the remote ID of the specific ports to bind with the specific Option 82 profile with a maximum of 32 characters.
NAME	Specifies the profile name.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to configure the per interface’s vendor defined string for Option 82 information remote ID sub-option.

Example

This example shows how to define vendor 3 remote-id format string as “switch1” on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip dhcp relay information option format-type remote-id vendor3 string
switch1
Switch(config-if)#
```

20-12 ip dhcp relay information option format circuit-id

This command is used to configure the DHCP information circuit ID sub-option. Use the **no** form of this command to configure the default circuit ID sub-option.

ip dhcp relay information option format circuit-id {default | string *STRING* **| vendor1 | vendor2 | vendor3 | vendor4 | vendor5 | vendor6 | expert-udf [{standalone_unit_format {0 | 1}}]}**

no ip dhcp relay information option format circuit-id

Parameters

default — Specifies to use the default circuit ID sub-option. If configured, the circuit ID will use the original format:

a.	b.	c.	d.	e.	f.	g.
1	0x6	0	4	VLAN	Module ID	Port ID
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

a. *Sub-option type:* The number 1 indicates that this is the circuit ID.

b. *Length:* The length of the value. This should be 6.

c. *Circuit ID’s sub-option:* This should be 0.

d. *Sub-option’s length*: This should be 4.

e. The VLAN ID (S-VID).

f. *Module ID:* For a stand-alone switch, this is 0. For a stacked switch, this is the box ID.

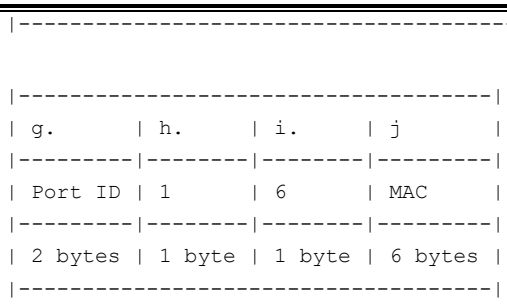
g. *Port ID:* Port number for each box.

STRING — Specifies to use a user-defined string as the circuit ID. Space characters are allowed in the string.

a.	b.	c.	d.	e.
2	n+2	1	n	User Defined
1 byte	1 byte	1 byte	1 byte	Max. 32 bytes

vendor1 — Specifies to use vender1. If configured, the circuit ID will use the following format to communicate with the server:

a.	b.	c.	d.	e.	f.
1	0x10	0	6	VLAN	Slot ID
1 byte	1 byte	1 byte	1 byte	2 bytes	2 bytes



a. *Sub-option type:* 1 means circuit ID.

b. *Length*.

c. *Circuit ID's sub-option's first tag:* This should be 0.

d. *First tag's length:* This should be 6.

e. *VLAN ID*.

f. *Slot ID:* For a stand-alone switch, this is 1. For a stacked switch, this is the box ID assigned by stacking.

g. *Port ID:* The port number of each box.

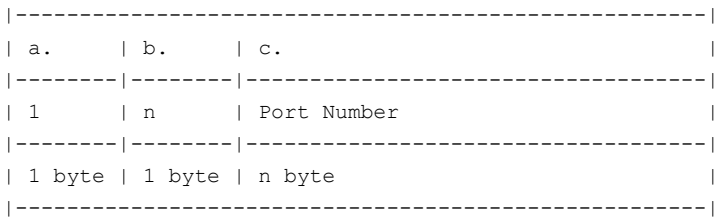
h. *Circuit ID's sub-option's second tag:* This should be 1.

i. *Second tag's length:* This should be 6.

j. *MAC address:* The Switch's system MAC address.

vendor2

Specifies to use vender2. If configured, the circuit ID will use the following format to communicate with the server:



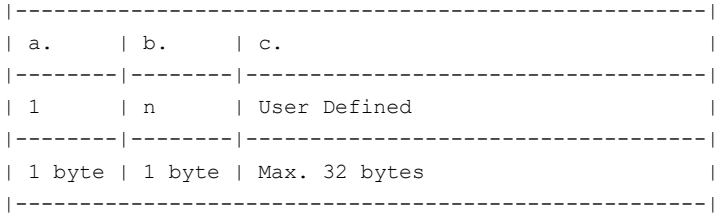
a. *Sub-option type:* 1 means circuit ID.

b. *Length:* The length of the value.

c. *Value:* The character string. The incoming port number of the DHCP client packet is formed in the string format and starts with the character "p". For example, "p02" means port 2. (When there is no circuit ID sub-option type, the value is directly filled in.) For the stacking port number, the format of port 1 on the switch unit 3 is p129. The maximum port number reserved for one switch unit is 64.

vendor3

Specifies to use vender3. If configured, the circuit ID will use the following format to communicate with the server:



a. *Sub-option type:* 1 means circuit ID.

b. *Length:* Total length of user-defined string. By default, Length is 0 and no value field.

c. *Value:* Flexible user-defined string that configured through the **ip dhcp relay information option format-type remote-id vendor3 string** *STRING* command. The maximum length is 32. (When there is no circuit ID sub-option type, the value is directly filled in.)

vendor4

Specifies to use vender4. If configured, the circuit ID will use the following format to communicate with the server:

a.	b.	c.	d.	e.	f.	g.	h.
1	n	System Name	-	Module ID	/	Port ID	-
1 byte	1 byte	0 to 128 bytes	1 byte	1 byte	1 byte	1 to 2 bytes	1 byte

i.
CVID
1 to 4 bytes

a. *Sub-option type:* 1 means circuit ID.

b. *Length:* Total length of all the following fields.

c. *System Name*.

d. *Separate Character*.

e. *Module ID:* For a standalone switch, the module ID is always 1. For a stacked switch, the module ID is the unit ID.

f. *Separate Character*.

g. *Port ID:* The port number of each box.

h. *Separate Character*.

i. *CVID:* This is client VLAN ID. When Q-in-Q is enabled, this is inner VLAN. Otherwise, it is outer VLAN.

vendor5

Specifies to use vender5. If configured, the circuit ID will use the following format to communicate with the server:

a.	b.	c.	d.	e.	f.	g.	h.
1	n	System Name	space (0x20)	e (0x65)	t (0x74)	h (0x68)	space (0x20)
1 byte	1 byte	0 to 128 bytes	1 byte	1 byte	1 byte	1 byte	1 byte

i.	j.	k.	l.	m.	n.	o.
Chassis ID	/ (0x2F)	Slot ID	/ (0x2F)	Port Number	: (0x3A)	VLAN ID
1 to 2 bytes	1 byte	1 to 2 bytes	1 byte	1 byte	1 byte	1 to 4 bytes

a. *Sub-option type:* 1 means circuit ID.

b. *Length*.

c. *System Name*: The system name of the Switch. If the system name exceeds 128 bytes, only the first 128 bytes will be used.

d. *Space*.

e. *e*: The ASCII code is 0x65..

f. *t:* The ASCII code is 0x74.

g. *h:* The ASCII code is 0x68.

h. *Space:* The ASCII code is 0x20.

i. *Chassis ID:* The number of the chassis. For a stand-alone device, this is 0. For a stacked device, this is the unit ID.

j. *Slash (/):* The ASCII code is 0x2F.

k. *Slot ID:* The number of the slot of the chassis. For a non-chassis device, this is the module ID of the device. The value starts from 0.

l. *Slash (/):* The ASCII code is 0x2F.

m. *Port Number*: the number of the client's port.

n. *Colon (:):*The ASCII code is 0x3A.

o. *VLAN ID*: the ID of the client's VLAN.

vendor6

Specifies to use vender6. If configured, the circuit ID will use the following format to communicate with the server:

F01	F02	F03	F04	F05	F06	F07	F08
1	Length	E	t	h	e	r	n
		(0x45)	(0x74)	(0x68)	(0x65)	(0x72)	(0x6E)
1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte	1 byte

F09	F10	F11	F12	F13	F14	F15	F16
e	t	Chassis ID	/	0	/	Port Number	:
(0x65)	(0x74)		(0x2F)	(0x30)	(0x2F)		(0x3A)
1 byte	1 byte	1 to 2 bytes	1 byte	1 byte	1 byte	1 to 2 bytes	1 byte

F17	F18	F19	F20	F21	F22	F23	F24
cvlan	.	0	Space	System Name	/	0	/
	(0x2E)	(0x30)	(0x20)		(0x2F)	(0x30)	(0x2F)
1 to 4 bytes	1 byte	1 byte	1 byte	1 to 128 bytes	1 byte	1 byte	1 byte

F25	F26	F27	F28	F29	F30	F31
0	/	Chassis ID	/	0	/	Port Number
(0x30)	(0x2F)		(0x2F)	(0x30)	(0x2F)	
1 byte	1 byte	1 to 2 bytes	1 byte	1 byte	1 byte	1 to 2 bytes

F01. *Sub-option type:* 1 means circuit ID.

F02. *Length*.

F03. *E:* The ASCII code is 0x45.

	F04. *t:* The ASCII code is 0x74. **F05.** *h:* The ASCII code is 0x68. **F06.** *e*: The ASCII code is 0x65. **F07.** *r:* The ASCII code is 0x72. **F08.** *n:* The ASCII code is 0x6E **F09.** *e:* The ASCII code is 0x65. **F10.** *t*: The ASCII code is 0x74. **F11.** *Chassis ID:* The number of the chassis. The format is ASCII string. For a standalone switch, the chassis ID is always 1. For a stacked switch, the chassis ID is the unit ID. **F12.** *Slash (/):* The ASCII code is 0x2F. **F13.** *0:* The ASCII code is 0x30. **F14.** *Slash (/):* The ASCII code is 0x2F. **F15.** *Port Number:* The incoming port number of the DHCP client packet. The format is ASCII string. **F16.** *Colon (:):*The ASCII code is 0x3A. **F17.** *cvlan:* The VLAN ID of the client. The value is from 1 to 4094. **F18.** *Dot (.):*The ASCII code is 0x2E. **F19.** *0:* The ASCII code is 0x30. **F20.** *Space:* The ASCII code is 0x20. **F21.** *System Name:* The system name of the Switch. If the system name exceeds 128 bytes, only the first 128 bytes will be used. **F22.** *Slash (/):* The ASCII code is 0x2F. **F23.** *0:* The ASCII code is 0x30. **F24.** *Slash (/):* The ASCII code is 0x2F. **F25.** *0:* The ASCII code is 0x30. **F26.** *Slash (/):* The ASCII code is 0x2F. **F27.** *Chassis ID:* The number of the chassis. The format is ASCII string. For a standalone switch, the chassis ID is always 1. For a stacked switch, the chassis ID is the unit ID. **F28.** *Slash (/):* The ASCII code is 0x2F. **F29.** *0:* The ASCII code is 0x30. **F30.** *Slash (/):* The ASCII code is 0x2F. **F31.** *Port Number*: The incoming port number of the DHCP client packet. The format is ASCII string.
expert-udf	Specifies to use expert-udf. If configures, use the user-defined string as the circuit ID: |---| | a. | b. | c. | |---| | 1 | n | User defined | |---| | 1 byte | 1 byte | Max. 251 bytes | |---| **a.** *Sub-option type:* The number 1 indicates that this is the circuit ID. **b.** *Length:* Total length of user-defined string. By default, Length is 0 and no value field. **c.** *Value:* Flexible user-defined string that configured through the **ip dhcp relay information option format-type circuit-id** and **ip dhcp relay information profile** commands. The maximum length is 251.
standalone_unit_format	(Optional) Specifies the unit ID for the standalone unit. The default value is 0.

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)#
```

20-13 ip dhcp relay information option format-type circuit-id

This command is used to configure the DHCP information circuit ID sub-option of the user-defined string. Use the **no** form of this command to remove the circuit ID sub-option.

ip dhcp relay information option format-type circuit-id {vendor3 string *STRING* **| expert-udf** *NAME***}**

no ip dhcp relay information option format-type circuit-id

Parameters

vendor3	Specifies to the vender3 user-defined string with the maximum 32 characters.
STRING	Specifies the profile name.
expert-udf	Specifies the remote ID of the specific ports to bind with the specific Option 82 profile with a maximum of 32 characters.
NAME	Specifies the profile name.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to configure each interface's vendor defined string for Option 82 information circuit ID sub-option.

Example

This example shows how to define vendor3 of "abc" on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)# ip dhcp relay information option format-type circuit-id vendor3 string abc
Switch(config-if)#
```

20-14 ip dhcp relay information trust-all

This command is used to enable the DHCP relay agent to trust the IP DHCP relay information for all interfaces. Use the **no** form of this command to disable the trusting on all interfaces.

ip dhcp relay information trust-all

no ip dhcp relay information trust-all

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When IP DHCP relay information trust is enabled on an interface, the arriving packets with a GIADDR of 0 (this relay agent is the first relay of this DHCP request packet) but with relay agent information option present will be accepted. If it is not trusted, these packets will be dropped.

When this command is enabled, IP DHCP relay information is trusted for all interfaces. When this command is disabled, the trust state is determined by the **ip dhcp relay information trusted** command in the Interface Configuration Mode.

Use the **show ip dhcp relay information trusted-sources** command to see the settings.

Example

This example shows how to enable the DHCP relay agent to trust IP DHCP relay information for all interfaces.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information trust-all
Switch(config)#
```

20-15 ip dhcp relay information trusted

This command is used to enable the DHCP relay agent to trust the relay information for the interface. Use the **no** form of this command to disable the trusting of relay information for the interface.

ip dhcp relay information trusted

no ip dhcp relay information trusted

Parameters

None.

Default

By default, information is not trusted.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When IP DHCP relay information trust is enabled on an interface, the arriving packets with a GIADDR of 0 (this relay agent is the first relay of this DHCP request packet) but with relay agent information option present will be accepted. If it is not trusted, these packets will be dropped.

When the **ip dhcp relay information trust-all** command is enabled, IP DHCP relay information is trusted for all interfaces. When the **ip dhcp relay information trust-all** command is disabled, the trust state is determined by this command.

Use the **show ip dhcp relay information trusted-sources** command to see the settings.

Example

This example shows how to disable the DHCP relay agent to trust all interface settings and enable trust for VLAN 100.

```
Switch#configure terminal
Switch(config)#no ip dhcp relay information trust-all
Switch(config)#interface vlan 100
Switch(config-if)#ip dhcp relay information trusted
Switch(config-if)#
```

20-16 ip dhcp local-relay vlan

This command is used to enable local relay on a VLAN or a group of VLANs. Use the **no** form of this command to disable the local relay function.

ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

no ip dhcp local-relay vlan *VLAN-ID* **[, | -]**

Parameters

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

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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.



NOTE: When the **ip dhcp relay** command is disabled on an interface, the interface will not relay or locally relay received DHCP packets.

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)#
```

20-17 ip dhcp smart-relay

This command is used to enable smart relay of the DHCP relay agent. Use the **no** form of this command to disable the function.

ip dhcp smart-relay

no ip dhcp smart-relay

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the received interface of the packet has secondary addresses, by default, the relay agent set the gateway address field of the packet to the primary address of the interface. When smart relay is enabled, the relay agent will count the number that a client retries sending of the DISCOVER message. The relay agent will change the gateway address to the secondary address of the received interface after three retries.

Example

This example shows how to enable smart relay.

```
Switch#configure terminal
Switch(config)#ip dhcp smart-relay
Switch(config)#
```

20-18 option hex (DHCP Relay)

This command is used to specify a DHCP option matching pattern for a DHCP class. Use the **no** form of this command to delete the specified matching pattern for a DHCP class.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Parameters

CODE	Specifies the DHCP option number.
PATTERN	Specifies the hexadecimal pattern of the specified DHCP option. The length of the pattern must be even-numbered.
*	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. The mask of every byte only supports 00 or FF.

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 to configure the DHCP class Service-A with DHCP Option 60 matching patterns 0x112233 and 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

This example shows how to configure the DHCP class Service-B with DHCP Option 60 matching patterns 0x5566 * and 0x5060 *.

```
Switch#configure terminal
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)#
```

This example shows how to configure the DHCP class Service-C with a DHCP Option 60 matching pattern 0x506007 with a bitmask of 00FF00.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-C
Switch(config-dhcp-class)#option 60 hex 506007 bitmask 00FF00
Switch(config-dhcp-class)#
```

20-19 relay destination

This command is used to specify the DHCP relay destination IP address associated with a relay pool. Use the **no** form of this command to delete a DHCP relay destination from the DHCP relay pool.

relay destination *IP-ADDRESS*

no relay destination *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the relay destination DHCP server IP address.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The relay destination of the DHCP server can be specified in the DHCP relay pool. To do this, use the **ip dhcp pool** command to enter the DHCP Pool Configuration Mode and then use the **relay source** command to specify the source subnet of the client requests. Use the **relay destination** command to specify the relay destination server address. Multiple relay sources and multiple relay destinations can be specified in a pool. If a packet matches 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 to create a DHCP relay pool “pool1”. 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)#
```

20-20 relay source

This command is used to specify the source subnet of client packets. Use the **no** form of this command to remove the source subnet

relay source *IP-ADDRESS SUBNET-MASK*

no relay source *IP-ADDRESS SUBNET-MASK*

Parameters

IP-ADDRESS	Specifies the source subnet of client packets.
SUBNET-MASK	Specifies the network mask of the source subnet.

Default

None.

Command Mode

DHCP Pool Configuration Mode.

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.

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)#
```

20-21 relay target

This command is used to specify a DHCP relay target for relaying packets that matches the value pattern of the option defined in the class. Use the **no** form of this command to delete a relay target.

relay target *IP-ADDRESS*

no relay target *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the relay target server IP address for the class.

Default

None.

Command Mode

DHCP Pool Class Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **class** command and this 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 when the interface that receives the packet has no IP address configured.

Example

This example shows how to configure a DHCP relay target for relaying packets that matches the value pattern of the option defined in the class.

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

20-22 service dhcp (DHCP Relay)

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, the state 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)#
```

20-23 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/Privileged EXEC 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

Total Entries: 5

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#
```

20-24 show ip dhcp relay information option format-type

This command is used to display the interface option format configuration.

show ip dhcp relay information option format-type [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the interface option format configuration. If no parameter is specified, information of all interfaces will be displayed.

Example

This example shows how to display the interface option format configuration.

```
Switch#show ip dhcp relay information option format-type

eth1/0/1
Remote ID vendor string: string1
eth1/0/2
Circuit ID vendor string: string1
eth1/0/3
Remote ID vendor string: string3
Circuit ID vendor string: string4

Total Entries: 3

Switch#
```

20-25 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/Privileged EXEC 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 display relay information Option 82 option and insert configuration information for all VLANs.

```
Switch#show ip dhcp relay information option-insert

Interface     Option-Insert
------------ ----------
vlan1         Enabled
vlan2         Disabled
vlan3         Not Configured

Total Entries: 3

Switch#
```

20-26 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/Privileged EXEC 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#
```

20-27 ip dhcp relay unicast

This command is used to configure the DHCP relay and local relay agent to process DHCP unicast packets. Use the **no** form of this command to not process DHCP unicast packets.

ip dhcp relay unicast

no ip dhcp relay unicast

Parameters

None.

Default

By default, DHCP client unicast packets will be relayed.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable the DHCP relay and local relay agent to process DHCP unicast packets.

Unicast includes all DHCP client message types like DHCP renew, release, and more. When several devices enable the relay state in the topology, the **unicast** state should be same. DHCP relay will not check if the VRRP role is master or slave when relaying the packet. It will always be relayed from the first relay agent because DHCP discovery cannot determine the VRRP master.

Example

This example shows how to enable the Switch to process DHCP client unicast packets.

```
Switch#configure terminal
Switch(config)#ip dhcp relay unicast
Switch(config)#
```

20-28 ip dhcp relay information profile

This command is used to define an Option 82 profile and enter the Option 82 Profile Configure mode. Use the **no** form of this command to delete the specified Option 82 profile.

ip dhcp relay information profile *PROFILE-NAME*

no ip dhcp relay information profile *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the profile name for defining Option 82 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 enter the Option 82 Profile Configure mode to define the Option 82 profile. The profile can be used to define the flexible user-defined Option 82 entry.

Example

This example shows how to enter the Option 82 Profile Configure mode to define the profile “remote_id”.

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#ip dhcp relay information profile remote_id
Switch(config-dhcp-profile)#
```

20-29 format string (DHCP Relay)

This command is used to add the entry of the flexible user-defined Option 82. Use the **no** form of this command to delete the entry of the flexible user-defined Option 82.

format string *FORMAT-STRING*

no format string

Parameters

FORMAT-STRING	Specifies the user-defined DHCP Option 82 format with a maximum of 255 characters. The rules that need to follow for this parameters are: • This parameter can be hexadecimal value, ASCII string, or any combination of hexadecimal value and ASCII string. An ASCII string needs to be enclosed with quotation marks (" "), such as "Ethernet"; Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in a packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "%" +"$"+"1-32"+"keyword"+":": **% -** Indicates that the string that follows this character is a formatted key string. **$** or **0** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either “$” or “0”, and cannot be specified as both at the same time. **$** indicates to fill leading space (0x20). **0** indicates to fill leading 0. To fill leading 0 (**0**) is the default setting. **1-32** - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. **keyword -** Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: **devtype:** The model name of device. Derived from the Module Name field in the **show version** command. Only an ASCII string is accepted. **sysname:** Indicates the System name of the Switch. The maximum length is 128. Only an ASCII string is accepted. **ifdescr:** Derived from ifDescr (IF-MIB). Only an ASCII string is accepted. **portmac:** Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of ASCII string, the MAC address format can be customized via special command (e.g., **ip dhcp relay information option mac-format case**). When in the format of a hexadecimal value, the MAC address will be encapsulated by order in hexadecimal. **sysmac:** Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands (e.g., **ip dhcp relay information option mac-format case**). When in the format of a hexadecimal value, the MAC address will be encapsulated by order in hexadecimal. **unit:** Indicates the unit ID. This can be ASCII string or hexadecimal value. For the standalone device, the unit ID is specified by the **ip dhcp relay information option format remote-id expert-udf [standalone_unit_format {0 | 1}]** command and the **ip dhcp relay information option format circuit-id expert-udf [standalone_unit_format {0 | 1}]** command. **module:** Indicates the module ID number. This can be either an ASCII string or a hexadecimal value. **port:** Indicates the local port number. This can be either an ASCII string or a hexadecimal value.

	svlan: Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value. **cvlan:** Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value. **: -** Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (:) can be ignored. The space (0x20) between **%** and **:** will be ignored. Other spaces will be encapsulated. • ASCII strings can be any combination of formatted key strings, 0-9, a-z, A-Z, !, @, #, $, %, ^, &, *, (,), _, +, |, -, =, \, [,], {, }, ;, :, ', ", /, ., ,, <, >, `, and space characters. **** is escape character. The special character after **** is the character itself. For example, **\%** is **%** itself, not the start indicator of a formatted key string. Space not in the formatted key string will also be encapsulated. • Hexadecimal values can be any combination of formatted key strings, 0-9, A-F, a-f, and space characters. The formatted key strings only support keywords which support hexadecimal value. Space not in the formatted key string will be ignored.

Default

None.

Command Mode

DHCP Profile Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the entry of the flexible user-defined Option 82.

Example

This example shows how to configure the entry of the flexible user-defined Option 82.

```
switch#configure terminal
switch(config)#ip dhcp relay information profile profile1
switch(config-dhcp-profile)#format string Ethernet "%unit:"/0/ "%port:"\:%sysname:"%05svlan
switch(config-dhcp-profile)#
```

20-30 ip dhcp relay information option mac-format case

This command is used to define the MAC address format of the Option 82 flexible user-defined profile. Use the **no** form of this command to revert to the default settings.

ip dhcp relay information option mac-format case {lowercase | uppercase} delimiter{hyphen | colon | dot | none } number {1 | 2 | 5}

no ip dhcp relay information option mac-format case

Parameters

lowercase	Specifies that when using the lowercase format, the Option 82 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff.

uppercase	Specifies that when using uppercase format, the Option 82 MAC address for the user-defined profile will be formatted as: AA-BB-CC-DD-EE-FF.
hyphen	Specifies that when using “-” as delimiter, the format is: AA-BB-CC-DD-EE-FF.
colon	Specifies that when using “:” as delimiter, the format is: AA:BB:CC:DD:EE:FF.
dot	Specifies that when using “.” as delimiter, the format is: AA.BB.CC.DD.EE.FF.
none	Specifies that when not using any delimiter, the format is: AABBCCDDEEFF.
number	Specifies the delimiter number value. Choose one of the following delimiter options: **1:** Single delimiter, the format is: AABBCC.DDEEFF. **2:** Double delimiters, the format is: AABB.CCDD.EEFF. **5:** Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF. If **none** is chosen for delimiter, the number does not take effect.

Default

The default authentication MAC address case is **uppercase**.

The default authentication MAC address delimiter is **none**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the MAC address format of the Option 82 flexible user-defined profile.

Example

This example shows how to configure the MAC address format of the Option 82 flexible user-defined profile.

```
Switch#configure terminal
Switch(config)#ip dhcp relay information option mac-format case uppercase delimiter hyphen
number 5
Switch(config)#
```

20-31 show ip dhcp relay information profile

This command is used to display the DHCP Option 82 profile configuration.

show ip dhcp relay information profile [*PROFILE-NAME***]**

Parameters

PROFILE-NAME	(Optional) Specifies the Option 82 profile name to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the DHCP Option 82 profile configuration.

Example

This example shows how to display the DHCP Option 82 profile configuration.

```
Switch#show ip dhcp relay information profile

Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"

Profile name: profile2
Format string: "Ethernet "%unit:"/0/  "%port:"\:%sysname:"%05svlan

Total Entries: 2

Switch#
```

20-32 show ip dhcp relay information option mac-format

This command is used to display the MAC address format of the Option 82 profile.

show ip dhcp relay information option mac-format

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the MAC address format of the Option 82 profile.

Example

This example shows how to display the MAC address format of the Option 82 profile.

```
Switch#show ip dhcp relay information option mac-format

 Case              : Uppercase
 Delimiter         : Hyphen
 Delimiter Number  : 5
 Example           : AA-BB-CC-DD-EE-FF

Switch#
```

20-33 ip dhcp relay

This command is used to enable the DHCP relay on the interface. Use the **no** form of this command to disable the function.

ip dhcp relay

no ip dhcp relay

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 and port-channel interface configuration.

Use this command to enable or disable the DHCP relay on the interface.

Example

This example shows how to enable the Switch to process DHCP client unicast packets.

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#interface eth1/0/2
Switch(config-if)#ip dhcp relay
Switch(config-if)#
```

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 this 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** command 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, 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 to create a DHCP class “Customer-A” 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 for the DHCP client to boot the device. Use the **no** form of this command to remove the specification of the boot file.

bootfile *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 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.cfg” as the name of the boot configuration file for DHCP pool 1.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#bootfile mdubootfile.cfg
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 {* | *IP-ADDRESS*}**

Parameters

all	Specifies to clear binding entries for all pools.
pool *NAME*	Specifies the name of the DHCP pool.
*	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 *, all automatic binding entries associated with the pool will be deleted. If **pool** is specified as all and the IP address is specified, 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, 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 pool2.

```
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 {* | *IP-ADDRESS*}**

Parameters

all	Specifies to clear conflict entries for all pools.
pool *NAME*	Specifies the name of the DHCP pool.
*	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 *, all conflict entries specific to the pool will be deleted. If **pool** is specified as all and the IP address is specified, 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, 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 Server)

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

class *NAME*

no class *NAME*

Parameters

NAME	Specifies the DHCP class name. 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 this 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.

Example

This example shows how to create two DHCP classes Customer-A and Customer-B 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 to configure a DHCP class Service-A and define it 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 172.19.18.0 255.255.255.0
Switch(config-dhcp-pool)#class Service-A
Switch(config-dhcp-pool-class)#relay target 10.2.1.2
Switch(config-dhcp-pool-class)#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** form of this 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 to create a DHCP address pool “pool1” with a manual binding entry which binds the IP address 10.1.2.3/24 with client ID 01524153203124.

```
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

Use this command to configure 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** form of this 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 to create a DHCP address pool “pool1” 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** form of this 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 to create a DHCP address pool “pool1” 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 Server)

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

ip dhcp class *NAME*

no ip dhcp class *NAME*

Parameters

NAME	Specifies the DHCP class name. 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 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 this command to remove a range of excluded addresses.

ip dhcp excluded-address *START-IP-ADDRESS END-IP-ADDRESS*

no ip dhcp excluded-address *START-IP-ADDRESS END-IP-ADDRESS*

Parameters

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 to exclude 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** form of this command to revert to the default setting.

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 revert to the default setting.

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 500 milliseconds (0.5 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 to create a DHCP address pool “pool1”.

```
Switch#configure terminal
Switch(config)#ip dhcp pool pool1
Switch(config-dhcp-pool)#
```

21-18 ip dhcp use class

This command is used to specify the DHCP server to use DHCP classes during address allocation. Use the **no** form of this 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 enable or disable the use of DHCP classes during address allocation.

Example

This example shows how to disable the use of DHCP classes.

```
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 revert to 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 or configuration file. 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** form of this command to remove the network.

network {*NETWORK-ADDRESS MASK* **|** *NETWORK-ADDRESS|PREFIX-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 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, 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 to configure the subnet 10.1.0.0/16 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	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, 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 Server)

This command is used to specify a DHCP option matching pattern for a DHCP class. Use the **no** form of this command to delete the specified matching pattern for a DHCP class.

option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

no option *CODE* **hex** *PATTERN* **[*] [bitmask** *MASK***]**

Parameters

CODE	Specifies the DHCP option number.
PATTERN	Specifies the hexadecimal pattern of the specified DHCP option. The length of the pattern must be even-numbered.
*	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. The mask of every byte only supports 00 or FF.

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 to configure the DHCP class Service-A with DHCP Option 60 matching patterns 0x112233 and 0x102030.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-A
Switch(config-dhcp-class)#option 60 hex 112233
Switch(config-dhcp-class)#option 60 hex 102030
Switch(config-dhcp-class)#
```

This example shows how to configure the DHCP class Service-B with DHCP Option 60 matching patterns 0x5566 * and 0x5060 *.

```
Switch#configure terminal
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)#
```

This example shows how to configure the DHCP class Service-C with a DHCP Option 60 matching pattern 0x506007 with a bitmask of 00FF00.

```
Switch#configure terminal
Switch(config)#ip dhcp class Service-C
Switch(config-dhcp-class)#option 60 hex 506007 bitmask 00FF00
Switch(config-dhcp-class)#
```

21-26 service dhcp (DHCP Server)

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, the state 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 [*IP-ADDRESS***]**

Parameters

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/Privileged EXEC 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

IP address          Client-ID/     Lease expiration    Type
                  Hardware address
 --------------- ----------------- -------------------- ---------
 10.0.0.1         01002211223344    Feb 25 2018 08:18 AM Automatic

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

IP address          Client-ID/     Lease expiration    Type
                  Hardware address
 --------------- ----------------- -------------------- ---------
 10.1.1.1         01002211223344    Feb 25 2018 08:21 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 [*IP-ADDRESS***]**

Parameters

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/Privileged EXEC 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, 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
 --------------- --------------- --------------------
 10.1.1.1        Ping            Oct 23 2013 09:12 AM

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
 --------------- --------------- --------------------
 10.1.1.1        Ping            Oct 23 2013 09:12 AM

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.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to examine the configuration settings of the pool. If no parameter is specified, information about all DHCP pools will be displayed.

Example

This example shows how to display the DHCP pool “pool1” configuration information.

```
Switch#show ip dhcp pool pool1

 Pool name: pool1
   Network: 10.0.0.0/8
   Boot file:
   Default router:
   DNS server:
   NetBIOS server:
   Domain name:
   Lease: 1 days 0 hours 0 minutes
   NetBIOS node type:
   Next server: 0.0.0.0
   Remaining unallocated address number: 1023
   Number of leased addresses: 1


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/Privileged EXEC 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: Disabled
 Ping packets number: 2
 Ping timeout: 500 ms
 Excluded Addresses
  10.0.1.1 - 10.1.1.1
 List of DHCP server configured address pool
  pool10  pool11  pool12  pool13  pool14  pool2  pool3  pool4  pool5  pool6  pool7  pool8
pool9

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/Privileged EXEC 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.

22. DHCP Server Screening Commands

22-1 based-on hardware-address

This command is used to add an entry of the DHCP server screen profile. Use the **no** form of this command to delete the specified entry.

based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

no based-on hardware-address *CLIENT-HARDWARE-ADDRESS*

Parameters

CLIENT-HARDWARE-ADDRESS	Specifies the MAC address of the client.

Default

None.

Command Mode

DHCP Server Screen Configure Mode.

Command Default Level

Level: 12.

Usage Guideline

The server message with the specified server IP address and client address in the payload will be permitted. These binding entries restrict that only specific servers are allowed to offer addresses to service specific clients.

Example

This example shows how to configure a DHCP server screen profile named “campus-profile” which contains a list of MAC addresses of clients.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#
```

22-2 clear ip dhcp snooping server-screen log

This command is used to clear the server screen log buffer.

clear ip dhcp snooping server-screen log

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

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#
```

22-3 dhcp-server-screen profile

This command is used to define a server screen profile and enter the DHCP Server Screen Configure Mode. Use the **no** form of this command to delete the specified server screen profile.

dhcp-server-screen profile *PROFILE-NAME*

no dhcp-server-screen profile *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the profile name with a maximum of 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the DHCP Server Screen Configure Mode to define a server screen profile. The profile can be used to define the DHCP server screen entry.

Example

This example shows how to enter the DHCP Server Screen Configure Mode to define the profile “campus”.

```
Switch#configure terminal
Switch(config)#service dhcp
Switch(config)#dhcp-server-screen profile campus
Switch(config-dhcp-server-screen)#
```

22-4 ip dhcp snooping server-screen

This command is used to enable DHCP server screening. Use the **no** form of this command to disable it.

ip dhcp snooping server-screen [*SERVER-IP-ADDRESS* **profile** *PROFILE-NAME***]**

no ip dhcp snooping server-screen [*SERVER-IP-ADDRESS***]**

Parameters

SERVER-IP-ADDRESS	(Optional) Specifies the trust DHCP sever IP address.
profile *PROFILE-NAME*	(Optional) Specifies the profile with the client MAC address list for the DHCP sever.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

The DHCP server screening function is used to filter the DHCP server packets on the specific interface and receive the trust packets from the specific source. This feature can make a protected network usable when a malicious host sends DHCP server packets.

If the server IP address is not specified, it will enabled or disabled the DHCP server screen on the interface. By default, the DHCP server screen is disabled on all interfaces. If enabled, the DHCP server screen, on a specific interface, will filter all DHCP server packets from the interface and only forward trusted server packets.

If a server screen entry is defined with a profile that contains a client MAC address, the server message with the server IP address and the client addresses contained in the profile is forwarded.

If an entry is defined without the client’s MAC address, the server message with the specified server IP address will be forwarded. Each server can only have one corresponding entry in the table.

If the entry is defined with a profile but the entry does not exist, messages with the server IP specified by the entry are not forwarded.

Example

This example shows how to configure a DHCP server screen profile named “campus-profile” and associate it with a DHCP server screen entry on port 3.

```
Switch#configure terminal
Switch(config)#dhcp-server-screen profile campus-profile
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-02-03-04
Switch(config-dhcp-server-screen)#based-on hardware-address 00-08-01-03-00-01
Switch(config-dhcp-server-screen)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping server-screen 10.1.1.2 profile campus-profile
Switch(config-if)#
```

22-5 ip dhcp snooping server-screen log-buffer

This command is used to configure the DHCP server screen log buffer parameter. Use the **no** form of this command to revert to the default setting.

ip dhcp snooping server-screen log-buffer entries *NUMBER*

no ip dhcp snooping server-screen log-buffer entries

Parameters

NUMBER	Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

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, 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)#
```

22-6 show ip dhcp server-screen log

This command is used to display the server screen log buffer.

show ip dhcp server-screen log

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

22-7 snmp-server enable traps dhcp-server-screen

This command is used to enable the sending of SNMP notifications for forged DHCP server attacking. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps dhcp-server-screen

no snmp-server enable traps dhcp-server-screen

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When DHCP server screening is enabled and if the Switch received a forged DHCP server packet, the Switch will log the event if any attack packet is received. Use this command to enable or disable the sending of SNMP notifications for such events.

Example

This example shows how to enable the sending of traps for DHCP server screening.

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

23. DHCP Snooping Commands

23-1 ip dhcp snooping

This command is used to globally enable DHCP snooping. Use the **no** form of this command to disable DHCP snooping.

ip dhcp snooping

no ip dhcp snooping

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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)#
```

23-2 ip dhcp snooping information option allow-untrusted

This command is used to globally allow DHCP packets with the relay Option 82 on the untrusted interface. Use the **no** form of this command to not allow packets with the relay Option 82.

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

Parameters

None.

Default

By default, this option is 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)#
```

23-3 ip dhcp snooping database

This command is used to configure the storing of DHCP snooping binding entries to a remote site. Use the **no** form of this command to disable the storing or revert the parameters to the default settings.

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: • tftp://location/filename
write-delay *SECONDS*	Specifies the time delay to write the entries after a change is seen in the binding entry. The default is 300 seconds. The range is from 60 to 86400.

Default

By default, the URL for the database agent is not defined.

The write delay value is set to 300 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to store the DHCP binding entry to a remote server. Use the follow methods to store DHCP binding entries:

- **tftp:** Store the entries to remote site via TFTP.

The lease time of the entry will not be modified and the live time will continue to be counted while the entry is provisioned.

Example

This example shows how to store the binding entry to a file in the file system.

```
Switch#configure terminal
Switch(config)#ip dhcp snooping database tftp: //10.0.0.2/store/dhcp-snp-bind
Switch(config)#
```

23-4 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#
```

23-5 clear ip dhcp snooping binding

This command is used to clear the DHCP binding entry.

clear ip dhcp snooping binding [*MAC-ADDRESS***] [***IP-ADDRESS***] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID***]**

Parameters

MAC-ADDRESS	(Optional) Specifies the MAC address to clear.
IP-ADDRESS	(Optional) Specifies the IP address to clear.

vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to clear.
interface *INTERFACE-ID*	(Optional) Specifies the interface to clear.

Default

None.

Command Mode

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#
```

23-6 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. The URL format can be: • tftp://location/filename

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.

The DHCP snooping binding entries can be loaded by using the following methods:

- **tftp:** Load the entries from remote site via TFTP.

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#
```

23-7 ip dhcp snooping binding

This command is used to manually configure a DHCP snooping entry.

ip dhcp snooping binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **expiry** *SECONDS*

Parameters

MAC-ADDRESS	Specifies the MAC address of the entry.
vlan *VLAN-ID*	Specifies the VLAN of the entry.
IP-ADDRESS	Specifies the IP address of the entry.
interface *INTERFACE-ID*	Specifies the interfaces to be configured.
expiry *SECONDS*	Specifies the interval after which bindings are no longer valid. This value must be between 60 and 4294967295 seconds.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to create a dynamic DHCP snooping entry.

Example

This example shows how to configure a DHCP snooping entry with IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 and port 10 with an expiry time of 100 seconds.

```
Switch#ip dhcp snooping binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10 expiry
100
Switch#
```

23-8 ip dhcp snooping trust

This command is used to configure a port as a trusted interface for DHCP snooping. Use the **no** form of this command to revert to the default setting.

ip dhcp snooping trust

no ip dhcp snooping trust

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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 the **ip dhcp snooping verify mac-address** command is enabled, the source MAC in the Ethernet header must be the same as the DHCP client hardware address to pass the validation.
- The untrusted interface receives a DHCP packet that includes a relay agent IP address that is not 0.0.0.0 or the relay agent forward a packet that includes Option 82 to an untrusted interface.
- The router receives a DHCPRELEASE or DHCPDECLINE message from an untrusted host with an entry in the DHCP snooping binding table, and the interface information in the binding table does not match the interface on which the message was received.

In addition to doing the validation, DHCP snooping also create a binding entry based on the IP address assigned to client by the server in DHCP snooping binding database. The binding entry contains information including MAC address, IP address, the VLAN ID and port ID where the client is located, and the expiry of the lease time.

Example

This example shows how to enable DHCP snooping trust for port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping trust
Switch(config-if)#
```

23-9 ip dhcp snooping limit entries

This command is used to configure the number of the DHCP snooping binding entries that an interface can learn. Use the **no** form of this command to reset the DHCP message entry limit.

ip dhcp snooping limit entries {*NUMBER* **| no-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 no-limit.

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 1 to 100.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip dhcp snooping limit entries 100
Switch(config-if)#
```

23-10 ip dhcp snooping limit rate

This command is used to configure the number of the DHCP messages that an interface can receive per second. Use the **no** form of this command to reset the DHCP message rate limiting.

ip dhcp snooping limit rate {*VALUE* **| no-limit}**

no ip dhcp snooping limit rate

Parameters

VALUE	Specifies the number of DHCP messages that can be processed per second. The valid range is from 1 to 300.
no-limit	Specifies no limitation on the rate.

Default

By default, this option is no-limit.

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.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ip dhcp snooping limit rate 100
Switch(config-if)#
```

23-11 ip dhcp snooping station-move deny

This command is used to disable the DHCP snooping station move state. Use the **no** form of this command to enable the DHCP snooping roaming state.

ip dhcp snooping station-move deny

no ip dhcp snooping station-move deny

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

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)#
```

23-12 ip dhcp snooping verify mac-address

This command is used to enable the verification that the source MAC address in a DHCP packet matches the client hardware address. Use the **no** form of this command to disable the verification of the MAC address.

ip dhcp snooping verify mac-address

no ip dhcp snooping verify mac-address

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

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)#
```

23-13 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-ID	Specifies the VLAN to enable or disable the DHCP snooping function.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, 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)#
```

23-14 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/Privileged EXEC 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
Station move is permitted.
Information option is not allowed on un-trusted interface

Interface      Trusted   Rate Limit   Entry Limit
-------------- --------- ------------ ------------
eth1/0/1       no        10           no_limit
eth1/0/2       no        50           no_limit
eth1/0/3       yes       no_limit     no_limit

Switch#
```

23-15 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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries by IP 10.1.1.1.

```
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    eth1/0/5

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  eth1/0/5

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  eth1/0/5

Total Entries: 1

Switch#
```

This example shows how to display DHCP snooping binding entries by VLAN 100.

```
Switch#show ip dhcp snooping binding vlan 100

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       1495           dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

This example shows how to display DHCP snooping binding entries on port 5.

```
Switch#show ip dhcp snooping binding interface eth1/0/5

MAC Address       IP Address      Lease(seconds) Type          VLAN Interface
----------------- --------------- -------------- ------------- ---- --------------
00-01-02-03-04-05 10.1.1.10       1500           dhcp-snooping 100  eth1/0/5
00-01-02-00-00-05 10.1.1.11       495            dhcp-snooping 100  eth1/0/5

Total Entries: 2

Switch#
```

Display Parameters

MAC Address	The client hardware MAC address.
IP Address	The client IP address assigned from the DHCP server.
Lease (seconds)	The IP address lease time.
Type	The Binding type configured from the CLI or dynamically learned.
VLAN	The VLAN ID.
Interface	The interface that connects to the DHCP client host.

23-16 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/Privileged EXEC 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.

24. DHCPv6 Client Commands

24-1 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 is only available for VLAN interface configuration.

This command restarts the IPv6 DHCP client on the specified interface.

Example

This example shows how to restart the DHCPv6 client for VLAN 1.

```
Switch#clear ipv6 dhcp client vlan1
Switch#
```

24-2 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] | hint** *IPV6-PREFIX***}**

no ipv6 dhcp client pd

Parameters

PREFIX-NAME	Specifies the IPv6 general prefix name with a maximum of 12 characters.
rapid-commit	(Optional) Specifies to use a two-message exchange instead of the standard four-message exchange between the Requesting Router (RR) and the Delegating Router (DR) to obtain the network configuration settings from the DHCPv6 Server.
hint *IPV6-PREFIX*	Specifies the IPv6 prefix to be sent in the message as a hint.

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.

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

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

If the **hint** parameter is specified for the command, the specified hint prefix will be included in the transmitted solicit or request message as a hint to the prefix delegation server. Only one hint prefix can be configured.

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)#
```

24-3 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	(Optional) Specifies the VLAN interface to display the DHCPv6 related settings.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use the **show ipv6 dhcp** command to display the device's DHCPv6 DUID.

Use the **show ipv6 dhcp interface** command to display DHCPv6 related setting for interfaces. If the interface ID is not specified, all interfaces with the DHCPv6 function will be displayed.

Example

This example shows how to display the DHCPv6 DUID for the device.

```
Switch#show ipv6 dhcp

This device's DUID is 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 lifetime 80, valid lifetime 100
  Prefix name: yy
  Rapid-Commit: disabled

Switch#
```

25. DHCPv6 Guard Commands

25-1 ipv6 dhcp guard policy

This command is used to create or modify a DHCPv6 guard policy, and enter the DHCPv6 Guard Policy Configuration Mode. Use the **no** form of this command to remove the DHCPv6 guard policy.

ipv6 dhcp guard policy *POLICY-NAME*

no ipv6 dhcp guard policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the DHCPv6 guard policy name.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create or modify the DHCPv6 guard policy, and enter the DHCPv6 Guard Policy Configuration Mode. DHCPv6 guard policies can be used to block DHCPv6 reply and advertisement messages that come from unauthorized servers. Client messages are not blocked.

After the DHCPv6 guard policy was created, use the **ipv6 dhcp guard attach-policy** command to apply the policy on a specific interface.

Example

This example shows how to create a DHCPv6 guard policy.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp guard policy policy1
Switch(config-dhcp-guard)#
```

25-2 device-role

This command is used to specify the role of the attached device. Use the **no** form of this command to revert to the default setting.

device-role {client | server}

no device-role

Parameters

client	Specifies that the attached device is a DHCPv6 client. All DHCPv6 server messages are dropped on this port.

server	Specifies that the attached device is a DHCPv6 server. DHCPv6 server messages are allowed on this port.

Default

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

Command Mode

DHCPv6 Guard Policy Configuration Mode.

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 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)#
```

25-3 match ipv6 access-list

This command is used to verify the sender's IPv6 address in server messages. Use the **no** form of this command to disable the verification.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*

no match ipv6 access-list

Parameters

IPV6-ACCESS-LIST-NAME	Specifies the IPv6 access list to be matched.

Default

By default, this option is disabled.

Command Mode

DHCPv6 Guard Policy Configuration Mode.

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)#
```

25-4 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 port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 dhcp guard attach-policy pol1
Switch(config-if)#
```

25-5 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no parameter is specified, information of all policies is displayed.

Example

This example shows how to displayed information of all policies.

```
Switch#show ipv6 dhcp guard policy

DHCP guard policy: default
   Device Role: DHCP client
   Target: eth1/0/3

DHCP guard policy: test1
   Device Role: DHCP server
   Source Address Match Access List: acl1
   Target: eth1/0/1

Switch#
```

Display Parameters

Device Role	The role of the device. The role is either client or server.
Target	The name of the target. The target is an interface.
Source Address Match Access List	The IPv6 access list of the specified policy.

26. DHCPv6 Relay Commands

26-1 ipv6 dhcp relay destination

This command is used to enable the DHCP for IPv6 relay service on the interface and specify a destination address to which client messages are forwarded to. Use the **no** form of this command to remove a relay destination.

ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

no ipv6 dhcp relay destination *IPV6-ADDRESS* **[***INTERFACE-ID***]**

Parameters

IPV6-ADDRESS	Specifies the DHCPv6 relay destination address.
INTERFACE-ID	(Optional) Specifies the output interface for the relay destination.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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.

```
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)#
```

26-2 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 setting.

ipv6 dhcp relay remote-id format {default | cid-with-user-define | user-define | expert-udf [standalone_unit_format {0 | 1}]}

no ipv6 dhcp relay remote-id format

Parameters

default — Specifies to use the Switch's system MAC address as the remote ID. The remote ID is formed in the following format:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	MAC Address
1 byte	2 bytes	1 byte	1 byte	6 bytes

F01. *Sub Type:* The number 1 indicates that this is the remote ID.

F02. *VLAN ID:* The incoming VLAN ID of the DHCP client packet.

F03. *Module ID:* For a standalone switch, the module ID is always 0. For a stacked switch, the module ID is the unit ID.

F04. *Port ID*: The incoming port number of the DHCP client packet. The port number starts from 1.

F05. *MAC Address*: The system MAC address of the Switch.

cid-with-user-define — Specifies to use a CID with user-defined string as the remote ID. The remote ID option is formed in the following format:

F01	F02	F03	F04	F05
Sub Type	VLAN ID	Module ID	Port ID	User Defined
1 byte	2 bytes	1 byte	1 byte	Max. 256 bytes

F01. *Sub Type:* The number 2 indicates that this is the remote ID.

F02. *VLAN ID:* The incoming VLAN ID of the DHCP client packet.

F03. *Module ID:* For a standalone switch, the module ID is always 0. For a stacked switch, the module ID is the unit ID.

F04. *Port ID*: The incoming port number of the DHCP client packet. The port number starts from 1.

F05. *User Defined*: The user-defined string configured in the **ipv6 dhcp relay remote-id udf** command. By default, the field is empty.

user-define — Specifies to use a user-defined string as the remote ID. The remote ID option is formed in the following format:

F01	F02
Sub Type	User Defined
1 byte	Max. 256 bytes

	F01. *Sub Type:* The number 3 indicates that this is the remote ID. **F02.** *User Defined*: The user-defined string configured in the **ipv6 dhcp relay remote-id udf** command.

expert-udf	Specifies to use a flexible user-defined string as the remote ID. The remote ID option is formed in the following format:
	`|----------------|`
	`| F01 |`
	`|----------------|`
	`| User Defined |`
	`|----------------|`
	`| Max. 256 bytes |`
	`|----------------|`
	
	F01. *User Defined*: The flexible user-defined string configured in the **ipv6 dhcp relay remote-id format-type**, **ipv6 dhcp relay remote-id profile**, and **format string** commands. By default, the field is empty.

standalone_unit_format	Specifies the unit ID for the standalone unit. The default value is 0.

Default

By default, the format for the DHCPv6 replay remote ID is **default**.

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)#
```

26-3 ipv6 dhcp relay remote-id option

This command is used to enable the insertion of the relay agent remote ID Option 37 during the relay of DHCP for IPv6 request packets. Use the **no** form of this command to disable the insert function.

ipv6 dhcp relay remote-id option

no ipv6 dhcp relay remote-id option

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable or disable the insertion of the DHCPv6 relay agent Remote ID option function.

Example

This example shows how to enable the insertion of the DHCPv6 relay agent remote ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id option
Switch(config)#
```

26-4 ipv6 dhcp relay remote-id policy

This command is used to configure the Option 37 forwarding policy for the DHCPv6 relay agent. Use the **no** form of this command to revert to the default setting.

ipv6 dhcp relay remote-id policy {drop | keep}

no ipv6 dhcp relay remote-id policy

Parameters

drop	Specifies to discard the packet that already has the relay agent Remote-ID Option 37.
keep	Specifies that the DHCPv6 request packet that already has the relay agent Remote-ID option is left unchanged and directly relayed to the DHCPv6 server.

Default

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

Command Mode

Global Configuration Mode.

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** parameter is used, relay agent's Remote ID option that has already been presented in the received packet from client, the packet will be dropped. If the **keep** parameter is used, the Switch does not check if there is a relay agent Remote-ID option in the received packet.

Example

This example shows how to configure the policy of the DHCPv6 relay agent Remote ID option to dropping the packet if it has a relay agent Remote-ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id policy drop
Switch(config)#
```

26-5 ipv6 dhcp relay remote-id udf

This command is used to configure the User Define Field (UDF) for remote ID. Use the **no** form of this command to delete the UDF entry.

ipv6 dhcp relay remote-id udf {ascii *STRING* **| hex** *HEX-STRING***}**

no ipv6 dhcp relay remote-id udf

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)#
```

26-6 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/Privileged EXEC 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#
```

26-7 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/Privileged EXEC 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
  Insert : disabled
  Policy : keep
  Format : default
  UDF is ascii string

IPv6 DHCP relay interface-id
  Insert : enabled
  Policy : keep
  Format : default


Switch#
```

26-8 ipv6 dhcp relay interface-id format

This command is used to configure the sub-type of the interface ID. Use the **no** form of this command to revert to the default setting.

ipv6 dhcp relay interface-id format {default | cid | vendor1 | expert-udf [standalone_unit_format {0 | 1}]}

no ipv6 dhcp relay interface-id format

Parameters

default	Specifies to use the VLAN ID as the interface ID. The interface ID is formed in the following format: |-------------------------| | F01 | F02 |

Sub Type	VLAN ID
1 byte	2 bytes

F01. *Sub Type:* The number 1 indicates that this is the interface ID.

F02. *VLAN ID:* The incoming VLAN ID of the DHCP client packet.

cid

Specifies to use the CID as the interface ID. The interface ID option is formed in the following format:

F01	F02	F03	F04
Sub Type	VLAN ID	Module ID	Port ID
1 byte	2 bytes	1 byte	1 byte

F01. *Sub Type:* The number 2 indicates that this is the interface ID.

F02. *VLAN ID:* The incoming VLAN ID of the DHCP client packet.

F03. *Module ID:* For a standalone switch, the module ID is always 0. For a stacked switch, the module ID is the unit ID.

F04. *Port ID*: The incoming port number of the DHCP client packet. The port number starts from 1.

vendor1

Specifies to use vendor 1. If configures, the interface ID option is formed in the following format:

F01	F02	F03	F04	F05
E	t	h	e	r
(0x45)	(0x74)	(0x68)	(0x65)	(0x72)
1 byte	1 byte	1 byte	1 byte	1 byte

F06	F07	F08	F09	F10
n	e	t	Chassis ID	/
(0x6E)	(0x65)	(0x74)		(0x2F)
1 byte	1 byte	1 byte	1~2 byte	1 byte

F11	F12	F13	F14	F15
0	/	Port	:	cvlan
(0x30)	(0x2F)	Number	(0x3A)	
1 byte	1 byte	1~2 byte	1 byte	1~4 byte

F16	F17	F18	F19	F20
.	0	Space	System	/
(0x2E)	(0x30)	(0x20)	Name	(0x2F)

```
| 1 byte     | 1 byte     | 1 byte     | 1~128 byte | 1 byte     |
|-------------------------------------------------------------------|

|-------------------------------------------------------------------|
| F21        | F22        | F23        | F24        | F25        |
|------------|------------|------------|------------|------------|
| 0          | /          | 0          | /          | Chassis ID |
| (0x30)     | (0x2F)     | (0x30)     |  (0x2F)    |            |
|------------|------------|------------|------------|------------|
| 1 byte     | 1 byte     | 1 byte     | 1 byte     | 1~2 byte   |
|-------------------------------------------------------------------|

|-------------------------------------------------|
| F26        | F27        | F28        | F29        |
|------------|------------|------------|------------|
| /          | 0          | /          | Port       |
| (0x2F)     | (0x30)     | (0x2F)     | Number     |
|------------|------------|------------|------------|
| 1 byte     | 1 bytes    | 1 byte     | 1~2 byte   |
|-------------------------------------------------|
```

F01. *E:* The ASCII code is 0x45.
F02. *t:* The ASCII code is 0x74.
F03. *h:* The ASCII code is 0x68.
F04. *e*: The ASCII code is 0x65.
F05. *r:* The ASCII code is 0x72.
F06. *n:* The ASCII code is 0x6E
F07. *e:* The ASCII code is 0x65.
F08. *t*: The ASCII code is 0x74.
F09. *Chassis ID:* The number of the chassis. For a standalone switch, the chassis ID is always 0. For a stacked switch, the chassis ID is the unit ID.
F10. *Slash (/):* The ASCII code is 0x2F.
F11. *0:* The ASCII code is 0x30.
F12. *Slash (/):* The ASCII code is 0x2F.
F13. *Port Number:* The incoming port number of the DHCP client packet.
F14. *Colon (:):*The ASCII code is 0x3A.
F15. *cvlan:* The VLAN ID of the client. The value is from 1 to 4094.
F16. *Dot (.):*The ASCII code is 0x2E.
F17. *0:* The ASCII code is 0x30.
F18. *Space:* The ASCII code is 0x20.
F19. *System Name:* The system name of the Switch.
F20. *Slash (/):* The ASCII code is 0x2F.
F21. *0:* The ASCII code is 0x30.
F22. *Slash (/):* The ASCII code is 0x2F.
F23. *0:* The ASCII code is 0x30.
F24. *Slash (/):* The ASCII code is 0x2F.
F25. *Chassis ID:* The number of the chassis. For a standalone switch, the chassis ID is always 0. For a stacked switch, the chassis ID is the unit ID.
F26. *Slash (/):* The ASCII code is 0x2F.
F27. *0:* The ASCII code is 0x30.
F28. *Slash (/):* The ASCII code is 0x2F.
F29. *Port Number*: The incoming port number of the DHCP client packet.

expert-udf	Specifies to use a flexible user-defined string as the interface ID. The interface ID option is formed in the following format: `|----------------|`

	<pre>| F01 | |----------| | User Defined | |----------| | Max. 255 bytes | |----------|</pre> **F01.** *User Defined*: The flexible user-defined string configured in the **ipv6 dhcp relay interface-id format-type expert-udf**, **ipv6 dhcp relay interface-id profile**, and **format string** commands. By default, the field is empty.
standalone_unit_format	Specifies the unit ID for the standalone unit. The default value is 0.

Default

By default, the format for the DHCPv6 replay interface ID is **default**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to configure the sub-type of the interface ID option.

Example

This example shows how to configure the sub-type of the remote ID to “cid”.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id format cid
Switch(config)#
```

26-9 ipv6 dhcp relay interface-id option

This command is used to enable the insertion of the relay agent interface ID Option 18 during the relay of DHCP for IPv6 request packets. Use the **no** form of this command to disable the insert function.

ipv6 dhcp relay interface-id option

no ipv6 dhcp relay interface-id option

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 the insertion of the DHCPv6 relay agent interface ID option function.

Example

This example shows how to enable the insertion of the DHCPv6 relay agent interface ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id option
Switch(config)#
```

26-10 ipv6 dhcp relay interface-id policy

This command is used to configure the Option 18 re-forwarding policy for the DHCPv6 relay agent. Use the **no** form of this command to revert to the default setting.

ipv6 dhcp relay interface-id policy {drop | keep}

no ipv6 dhcp relay interface-id policy

Parameters

drop	Specifies to discard the packet that already has the relay agent Interface-ID Option 18.
keep	Specifies that the DHCPv6 request packet that already has the relay agent Interface-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 18. If the **drop** policy is selected, relay agent's Interface 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 does not check if there is a relay agent Interface-ID option in the received packet.

Example

This example shows how to configure the policy of the DHCPv6 relay agent Interface ID option to drop the packet if it has a relay agent Interface-ID option.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id policy drop
Switch(config)#
```

26-11 ipv6 dhcp local-relay vlan

This command is used to enable DHCPv6 local relay on a VLAN or a group of VLANs. Use the **no** form of this command to disable the function.

ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**

no ipv6 dhcp local-relay vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the VLAN ID to be configured.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the DHCPv6 local relay function.

When DHCPv6 local relay is enabled, the Switch will add Option 37 and Option 18 to the request packets from the client.

If the Option 37 check state is enabled, the Switch will check the request packet from the client and drop the packet if it contains Option 37 as specified in the DHCPv6 relay function.

If the Option 37 check state is disabled, the local relay function will always add Option 37 to the request packet, regardless whether the state of Option 37 is enabled or disabled.

The DHCPv6 local relay function will directly forward the packet from the server to the client after which no more processing is done.



NOTE: When the **ipv6 dhcp relay enable** command is disabled on an interface, the interface will not relay or locally relay received DHCPv6 packets.

Example

This example shows how to enable the DHCPv6 local relay function on VLAN 100.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp local-relay vlan 100
Switch(config)#
```

26-12 ipv6 dhcp relay enable

This command is used to enable the DHCPv6 relay function per port. Use the **no** form of this command to disable the function.

ipv6 dhcp relay enable

no ipv6 dhcp relay enable

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 configure the state of the DHCPv6 relay function for each port.

Example

This example shows how to disable the DHCPv6 relay function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no ipv6 dhcp relay enable
Switch(config-if)#
```

26-13 ipv6 dhcp relay remote-id profile

This command is used to create a new profile for DHCPv6 relay Option 37 and enter the DHCPv6 Profile Configuration mode. Use the **no** form of this command to remove the profile.

ipv6 dhcp relay remote-id profile *NAME*

no ipv6 dhcp relay remote-id profile *NAME*

Parameters

NAME	Specifies the profile name. The maximum length is 32 characters. The profile can be created up to 6 entries.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create or remove a profile for DHCPv6 relay Option 37, or enter the DHCPv6 Profile Configuration mode.

Example

This example shows how to create a profile, profile1, for DHCPv6 relay Option 37.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay remote-id profile profile1
Switch(config-dhcp-profile)#
```

26-14 ipv6 dhcp relay interface-id profile

This command is used to create a new profile for DHCPv6 relay Option 18 and enter the DHCPv6 Profile Configuration Mode. Use the **no** form of this command to remove the profile.

ipv6 dhcp relay interface-id profile *NAME*

no ipv6 dhcp relay interface-id profile *NAME*

Parameters

NAME	Specifies the profile name. The maximum length is 32 characters. The profile can be created up to 6 entries.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create or remove a profile for DHCPv6 relay Option 18, or enter the DHCPv6 Profile Configuration Mode.

Example

This example shows how to a profile, profile2, for DHCPv6 relay Option 18.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id profile profile2
Switch(config-dhcp-profile)#
```

26-15 format string

This command is used to add the entry of the flexible user-defined Option 18 or Option 37. Use the **no** form of this command to delete the entry of the flexible user-defined Option 18 or Option 37.

format string *STRING*

no format string

Parameters

STRING	Specifies the user-defined DHCP Option 18 or Option 37 format with a maximum of 255 characters. The rules that need to follow for this parameters are: • This parameter can be hexadecimal value, ASCII string, or any combination of hexadecimal value and ASCII string. An ASCII string needs to be enclosed with quotation marks (" "), such as "Ethernet"; Any ASCII characters outside of the quotation marks will be interpreted as hexadecimal values. • A formatted key string is a string that should be translated before being encapsulated in a packet. A formatted key string can be contained both ASCII strings and hexadecimal values. For example, "%" +"$"+"1-32"+"keyword"+":": **% -** Indicates that the string that follows this character is a formatted key string. **$** or **0** - (Optional) Indicates a fill indicator. This option specifies how to fill the formatted key string to meet the length option. This option can be either “$” or “0”, and cannot be specified as both at the same time. **$** indicates to fill leading space (0x20). **0** indicates to fill leading 0. To fill leading 0 (**0**) is the default setting. **1-32** - (Optional) Indicates a length option. This specifies how many characters or bytes the translated key string should occupy. If the actual length of the translated key string is less than the length specified by this option, a fill indicator will be used to fill. Otherwise, this length option and fill indicator will be ignored and the actual string will be used directly. **keyword -** Indicates that the keyword will be translated based on the actual value of the system. The following keyword definitions specifies that a command will be refused if an unknown or unsupported keyword is detected: **devtype:** The model name of device. Derived from the Module Name field in the **show version** command. Only an ASCII string is accepted. **sysname:** Indicates the System name of the Switch. The maximum length is 128. Only an ASCII string is accepted.

ifdescr: Derived from ifDescr (IF-MIB). Only an ASCII string is accepted.

portmac: Indicates the MAC address of a port. This can be either an ASCII string or a hexadecimal value. When in the format of ASCII string, the MAC address format can be customized via special command (e.g., **ipv6 dhcp relay information option mac-format case**). When in the format of a hexadecimal value, the MAC address will be encapsulated by order in hexadecimal.

sysmac: Indicates the system MAC address. This can be either an ASCII string or a hexadecimal value. When in the format of an ASCII string, the MAC address format can be customized using special CLI commands (e.g., **ipv6 dhcp relay information option mac-format case**). When in the format of a hexadecimal value, the MAC address will be encapsulated by order in hexadecimal.

unit: Indicates the unit ID. This can be ASCII string or hexadecimal value. For the standalone device, the unit ID is specified by the **ipv6 dhcp relay remote-id format expert_udf [standalone_unit_format {0 | 1}]** command and the **ipv6 dhcp relay interface-id format expert_udf [standalone_unit_format {0 | 1}]** command.

module: Indicates the module ID number. This can be either an ASCII string or a hexadecimal value.

port: Indicates the local port number. This can be either an ASCII string or a hexadecimal value.

svlan: Indicates the outer VLAN ID. This can be either an ASCII string or a hexadecimal value.

cvlan: Indicates the inner VLAN ID. This can be either an ASCII string or a hexadecimal value.

: - Indicates the end of the formatted key sting. If a formatted key string is the last parameter of the command, its ending character (:) can be ignored. The space (0x20) between **%** and **:** will be ignored. Other spaces will be encapsulated.

- ASCII strings can be any combination of formatted key strings, 0-9, a-z, A-Z, !, @, #, $, %, ^, &, *, (,), _, +, |, -, =, \, [,], {, }, ;, :, ', ", /, ., ,, <, >, `, and space characters. **** is escape character. The special character after **** is the character itself. For example, **\%** is **%** itself, not the start indicator of a formatted key string. Space not in the formatted key string will also be encapsulated.
- Hexadecimal values can be any combination of formatted key strings, 0-9, A-F, a-f, and space characters. The formatted key strings only support keywords which support hexadecimal value. Space not in the formatted key string will be ignored.

Default

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

Command Mode

DHCPv6 Profile Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the entry of the flexible user-defined Option 18 or Option 37.

Example

This example shows how to configure the entry of the flexible user-defined Option 18.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay interface-id profile profile2
Switch(config-dhcp-profile)#format string "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"
Switch(config-dhcp-profile)#
```

26-16 ipv6 dhcp relay information option mac-format case

This command is used to define the MAC address format of the DHCPv6 Option 18 or Option 37 flexible user-defined profile. Use the **no** form of this command to revert to the default settings.

ipv6 dhcp relay information option mac-format case {lowercase | uppercase} delimiter {hyphen | colon | dot | none} number {1 | 2 | 5}

no ipv6 dhcp relay information option mac-format case

Parameters

lowercase	Specifies that when using the lowercase format, the Option 18 or Option 37 MAC address for the user-defined profile will be formatted as: aa-bb-cc-dd-ee-ff.
uppercase	Specifies that when using uppercase format, the Option 18 or Option 37 MAC address for the user-defined profile will be formatted as: AA-BB-CC-DD-EE-FF.
hyphen	Specifies that when using “-” as delimiter, the format is: AA-BB-CC-DD-EE-FF.
colon	Specifies that when using “:” as delimiter, the format is: AA:BB:CC:DD:EE:FF.
dot	Specifies that when using “.” as delimiter, the format is: AA.BB.CC.DD.EE.FF.
none	Specifies that when not using any delimiter, the format is: AABBCCDDEEFF.
number	Specifies the delimiter number value. Choose one of the following delimiter options: **1:** Single delimiter, the format is: AABBCC.DDEEFF. **2:** Double delimiters, the format is: AABB.CCDD.EEFF. **5:** Multiple delimiters, the format is: AA.BB.CC.DD.EE.FF. If none is chosen for delimiter, the number does not take effect.

Default

The default authentication MAC address case is **uppercase**.

The default authentication MAC address delimiter is **none**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the MAC address format of the DHCPv6 Option 18 or Option 37 flexible user-defined profile.

Example

This example shows how to specify the MAC address format of the Option 18 or Option 37 flexible user-defined profile.

```
Switch#configure terminal
Switch(config)#ipv6 dhcp relay information option mac-format case uppercase delimiter hyphen number 5
Switch(config)#
```

26-17 show ipv6 dhcp relay information option mac-format

This command is used to display the MAC address format of the Option 18 and Option 37 profile.

show ipv6 dhcp relay information option mac-format

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the MAC address format of the Option 18 and Option 37 profile.

Example

This example shows how to display the MAC address format of the Option 18 and Option 37 profile.

```
Switch#show ipv6 dhcp relay information option mac-format

 Case              : Uppercase
 Delimiter         : Hyphen
 Delimiter Number  : 5
 Example             : AA-BB-CC-DD-EE-FF

Switch#
```

26-18 ipv6 dhcp relay remote-id format-type expert-udf

This command is used to configure the Option 37 expert UDF string per port. Use the **no** form of this command to revert to the default setting.

ipv6 dhcp relay remote-id format-type expert-udf *STRING*

no ipv6 dhcp relay remote-id format-type

Parameters

STRING	Specifies the profile name of Option 37.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the Option 37 expert UDF string per port.

Example

This example shows how to configure the Option 37 on port 1 to use “profile1”.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 dhcp relay remote-id format-type expert-udf profile1
Switch(config-if)#
```

26-19 ipv6 dhcp relay interface-id format-type expert-udf

This command is used to configure the Option 18 expert UDF string per port. Use the **no** form of this command to revert to the default setting.

ipv6 dhcp relay interface-id format-type expert-udf *STRING*

no ipv6 dhcp relay interface-id format-type

Parameters

STRING	Specifies the profile name of Option 18.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the Option 18 expert UDF string per port.

Example

This example shows how to configure the Option 18 on port 1 to use “profile2”.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 dhcp relay interface-id format-type expert-udf profile2
Switch(config-if)#
```

26-20 show ipv6 dhcp relay interface-id profile

This command is used to display Option 18 profiles.

show ipv6 dhcp relay interface-id profile

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display Option 18 profiles.

Example

This example shows how to display Option 18 profiles.

```
Switch#show ipv6 dhcp relay interface-id profile

Option18 Profile name: profile2
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"


Total Entries:1

Switch#
```

26-21 show ipv6 dhcp relay remote-id profile

This command is used to display Option 37 profiles.

show ipv6 dhcp relay remote-id profile

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display Option 37 profiles.

Example

This example shows how to display Option 37 profiles.

```
Switch#show ipv6 dhcp relay remote-id profile

Option37 Profile name: profile1
Format string: "Ethernet %unit:/0/  %port:\:%sysname:%05svlan"


Total Entries:1

Switch#
```

27. DHCPv6 Server Commands

27-1 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 this parameter 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 this parameter is not specified, the default preferred 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)#
```

27-2 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 CLIENT-DUID* **[iaid** *IAID***]**

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 this parameter 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 this parameter 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, the match entry will be assigned. If there is no match entry but there are free static entries without IAID specified and match the DUID of the message, 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(config-dhcp)#address prefix 2001:0DB8::0/64 lifetime 200 100
Switch(config-dhcp)#address-assignment 2001:0DB8::1:2 000300010506BBCCDDEE
Switch(config-dhcp)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

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(config-dhcp)#address prefix 2001:AAB8::0/64 lifetime 200 100
Switch(config-dhcp)#address-assignment 2001:AAB8::2:2 00030001050611223344 iaid 1234
Switch(config-dhcp)#exit
Switch(config)#interface vlan200
Switch(config-if)#ipv6 dhcp server pool2
Switch(config-if)#
```

27-3 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#
```

27-4 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

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)#
```

27-5 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)#
```

27-6 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 this 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)#
```

27-7 ipv6 dhcp pool

This command is used to enter the DHCPv6 Pool Configuration Mode and configure the IPv6 DHCP pool. Use the **no** form of this 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 12 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the DHCPv6 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)#
```

27-8 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] [preference** *VALUE***] [allow-hint]**

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 use a two-message exchange instead of the standard four-message exchange between the Requesting Router (RR) and the Delegating Router (DR) to obtain the network configuration settings from the DHCP Server. By default, two-message exchange is not allowed.
preference *VALUE*	(Optional) Specifies the preference value to be advertised by the server The range is from 0 to 255. The default value is 0. the higher the value, the higher the priority.
allow-hint	(Optional) Specifies to delegate the prefix based on the prefix hint by the client. By default, the prefix hint by client is ignored.

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.

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

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

If the command is configured with a **preference** value other than 0, the preference value will be filled as option in the advertise message. An advertise message without the preference option is equivalent to having a preference value of 0. A higher preference represents a higher precedence.

If the command is configured with the **allow-hint** option, the server will delegate the prefix based on prefix hint by client. Otherwise, the prefix hint by client is ignored.

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)#
```

27-9 ipv6 local pool

This command is used to configure a local IPv6 prefix pool. Use the **no** form of this command 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 12 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)#
```

27-10 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 CLIENT-DUID* **[iaid** *IAID***]**

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 this parameter 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 this parameter 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, all the match entries will be delegated. If there are no match entries, but there are free static entries without IAID specified and match the DUID of the

message, the match entries are replied. If the request message has no IAID option, but there are free static entries without IAID specified and match the DUID of the message, 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 local pool prefix-pool 2001:DB8::/48 64
Switch(config)#ipv6 dhcp pool pool1
Switch(config-dhcp)#prefix-delegation pool prefix-pool lifetime 300 200
Switch(config-dhcp)#prefix-delegation 2001:0DB8::/64 000300010506BBCCDDEE
Switch(config-dhcp)#exit
Switch(config)#interface vlan 100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

27-11 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 this command to remove 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 this parameter 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 this parameter 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 “prefix-pool”, 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 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)#exit
Switch(config)#interface vlan100
Switch(config-if)#ipv6 dhcp server pool1
Switch(config-if)#
```

27-12 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 ipv6 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)#
```

27-13 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/Privileged EXEC 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 test
  Preference value: 0
  Hint from client: ignored
  Rapid-Commit is disabled

Switch#
```

27-14 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/Privileged EXEC 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 : 00030001aabbcd000001
                address: 1234::2
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000000
                address: 1234::3
                         preferred lifetime 200 ,valid lifetime 300

Client DUID : 00030001aabbcd000002
                address: 1234::4
                         preferred lifetime 200 ,valid lifetime 300


Total Entries: 3

Switch#
```

27-15 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/Privileged EXEC 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: pool1
        Static bindings:
           Binding for client 00030001aabbcd000080
           IA PD: IA ID 0x0001
              Prefix: 3000:0:300::/48
               preferred lifetime 604800, valid lifetime 2592000
        Prefix delegation pool: abc
              preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com
        Active clients: 0

DHCPv6 pool: pool2
        DNS server: 6000::2
        DNS server: 6000::9
        Domain name: pool2.com
        Active clients: 0

DHCPv6 pool: test
        Static bindings:
           Binding for client 00030001aabbcd001234
           IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        Address prefix: 1234::/64
              preferred lifetime 200, valid lifetime 300
        DNS server:
        Domain name:
        Active clients: 3

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.

27-16 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/Privileged EXEC 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 display the configured exclude addresses.

```
Switch#show ipv6 excluded-address

 IPv6 excluded address:
        1.      2000::123
        2.      2000::237 - 2000::333

 Total Entries: 2

Switch#
```

27-17 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/Privileged EXEC 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
------------ ----------------------------------------- ---- ------
prefix-pool  3004:DB8::/48                             65536 0
------------ ----------------------------------------- ---- ------
Total Entries: 1

Switch#
```

This example shows how to display the information for local pool called “PP1”.

```
Switch#show ipv6 local pool PP1

Prefix is 3004:DB8::/48 assign /64 prefix
1 entries in use, 65536 available, 0 rejected
User                 Prefix                                    Interface
-------------------- ----------------------------------------- ----------
000300010002FCA5C01C 2003::/64                                 vlan1

Switch#
```

27-18 show ipv6 dhcp operation

This command is used to display the operational information for the DHCPv6 server.

show ipv6 dhcp operation

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the operational information for the DHCPv6 server.

Example

This example shows how to display the operational information for the DHCPv6 server.

```
switch#show ipv6 dhcp operation

DHCPv6 pool: pool1
        Prefix delegation pool: abc, prefix is 3000::/32 48
        Static bindings:
           Binding for client 00030001aabbcd000080
             IA PD: IA ID 0x0001
             Prefix: 3000:0:300::/48
             preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 604800, valid lifetime 2592000
        DNS server: 2345::2
        Domain name: pool1.com

DHCPv6 pool: test
        Address prefix: 1234::/64
        Static bindings:
           Binding for client 00030001aabbcd001234
            IA NA: IA ID not specified
              Address: 1234::1234
               preferred lifetime 604800, valid lifetime 2592000
        preferred lifetime 200, valid lifetime 300
        DNS server: 2000::2
        Domain name: test.com

switch#
```

28. Digital Diagnostics Monitoring (DDM) Commands

28-1 show interfaces transceiver

This command is used to display the current SFP/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.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
detail	(Optional) Specifies to display more detailed information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the current SFP/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

Transceiver Monitoring traps: None

           Temperature  Voltage      Bias Current TX Power     RX Power
port       (Celsius)    (V)          (mA)         (mW/dbm)     (mW/dbm)
---------- ------------ ------------ ------------ ------------ ------------
eth1/0/21  30.845       3.284        7.895        0.604        0.470
                                                 -2.189       -3.279

Total Entries: 1

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.

eth1/0/21
 Transceiver Monitoring is enabled
 Transceiver Monitoring shutdown action: None

                 Current      High-Alarm   High-Warning Low-Warning  Low-Alarm
Temperature(C)   30.803       78.000       73.000       -8.000       -13.000
Voltage(V)       3.284        3.700        3.600        3.000        2.900
Bias Current(mA) 7.890        11.800       10.800       5.000        4.000
TX Power(mW)     0.604        0.832        0.661        0.316        0.251
         (dbm)   -2.191       -0.800       -1.800       -5.000       -6.000
RX Power(mW)     0.470        1.000        0.794        0.016        0.010
         (dbm)   -3.283       0.000        -1.000       -18.013      -20.000

Switch#
```

28-2 snmp-server enable traps transceiver-monitoring

This command is used to enable the sending of all or individual optical transceiver monitoring SNMP notifications. Use the **no** form of this command to disable the sending of all or individual optical transceiver monitoring SNMP notifications.

snmp-server enable traps transceiver-monitoring [alarm] [warning]

no snmp-server enable traps transceiver-monitoring [alarm] [warning]

Parameters

alarm	(Optional) Specifies to enable or disable the sending of alarm level notifications.
warning	(Optional) Specifies to enable or disable the sending of warning level notifications.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If no optional parameter is specified, it will enable or disable all transceiver-monitoring SNMP notifications.

Example

This example shows how to enable the sending of warning level notifications.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps transceiver-monitoring warning
Switch(config)#
```

28-3 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 this 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 port 27 when an alarm event is detected.

```
Switch#configure terminal
Switch(config)#interface eth1/0/27
Switch(config-if)#transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

28-4 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 this 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 is from 0 to 131 mA.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This configuration is only suitable for 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/SFP+ module.

If the SFP/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 port 27.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring bias-current eth1/0/27 high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

28-5 transceiver-monitoring enable

This command is used to enable the optical transceiver monitoring function for an SFP+ port. Use the **no** form of this command to remove 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/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/SFP+ transceiver'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 port 27.

```
Switch#configure terminal
Switch(config)#interface eth1/0/27
Switch(config-if)#transceiver-monitoring enable
Switch(config-if)#
```

28-6 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+ 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/SFP+ module.

If the SFP/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 port 27.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring rx-power eth1/0/27 low warning mwatt 0.135
Switch(config)#
```

28-7 transceiver-monitoring temperature

This command is used to configure the temperature thresholds for the specified port. Use the **no** form of this 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+ 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/SFP+ module.

If the SFP/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 port 27.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring temperature eth1/0/27 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

28-8 transceiver-monitoring tx-power

This command is used to configure the output power threshold for the specified port. Use the **no** form of this 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

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.
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+ 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/SFP+ module.

If the SFP/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 port 27.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring tx-power eth1/0/27 low warning mwatt 0.181
Switch(config)#
```

28-9 transceiver-monitoring voltage

This command is used to configure the threshold voltage of the specified port. Use the **no** form of this 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 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 0 and 6.55 Volt.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only 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/SFP+ module.

If the SFP/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 port 27.

```
Switch#configure terminal
Switch(config)#transceiver-monitoring voltage eth1/0/27 low alarm 0.005
Switch(config)#
```

29. Distance Vector Multicast Routing Protocol (DVMRP) Commands

29-1 ip dvmrp

This command is used to enable DVMRP on the current interface. Use the **no** form of this command 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 enabling the DVMRP function on an interface, IP multicast routing should be enabled by using the **ip multicast-routing** command in the Global Configuration Mode. Only one multicast routing protocol can be enabled on one interface. If more than one multicast routing protocol is enabled, 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
```

29-2 ip dvmrp metric

This command is used to configure the metric associated with the route for DVMRP reports. Use the **no** form of this command to revert to the default setting.

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
```

29-3 ip dvmrp neighbor-timeout

This command is used to configure the DVMRP neighbor lifetime value. Use the **no** form of this command to revert to the default setting.

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
```

29-4 ip dvmrp probe-time

This command is used to configure the DVMRP probe interval. Use the **no** form of this command to revert to the default setting.

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
```

29-5 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 VLAN interface.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

29-6 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/Privileged EXEC 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.

29-7 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display DVMRP route information.

Example

This example shows how to display 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     10.10.11.11        1       Local    vlan1      -      -

Total Entries: 1

Switch#
```

Display Parameters

Source Network	The source network.
Upstream neighbor	The next hop router to the source network. If the interface is a local entry, the upstream 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. The route state displays “-” if it is a local interface.
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).

30. D-Link Discovery Protocol (DDP) Client Commands

30-1 ddp

This command is used to enable DDP client function globally or on the specified ports. Use the **no** form of this command to disable DDP client.

ddp

no ddp

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable DDP client function globally or per physical port based.

When DDP is disabled on a port, the port will neither process nor generate DDP message. DDP messages received by the port are flooded in VLAN.

Example

This example shows how to enable DDP globally.

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

This example shows how to enable DDP on port 1.

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

30-2 ddp report-timer

This command is used to configure interval between two consecutive DDP report messages. Use the **no** form of this command to revert to the default setting.

ddp report-timer {30 | 60 | 90 | 120 | Never}

no ddp report-timer

Parameters

30	Specifies the report interval to 30 seconds.
60	Specifies the report interval to 60 seconds.
90	Specifies the report interval to 90 seconds.
120	Specifies the report interval to 120 seconds.
Never	Specifies to stop sending report message.

Default

By default, this option is **Never**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure interval between two consecutive DDP report messages.

Example

This example shows how to configure interval to 60 seconds.

```
Switch#configure terminal
Switch(config)#ddp report-timer 60
Switch(config)#
```

30-3 show ddp

This command is used to display DDP configurations of the Switch.

show ddp [interfaces *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

This example shows how to display DDP global information.

```
Switch#show ddp

D-Link Discovery Protocol state: Enabled
DDP Version:  5
Report timer: Never

Switch#
```

This example shows how to display DDP on port 1.

```
Switch#show ddp interface eth1/0/1

Interface          State
---------------    ----------
eth1/0/1           Enabled

Switch#
```

30-4 show ddp neighbors

This command is used to display the information of DDP neighbors.

show ddp neighbors [interface *INTERFACE-ID* **[, | -]] [detail]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the information of DDP neighbors.

Example

This example shows how to display the information of DDP neighbors.

```
Switch#show ddp neighbors
Total Entries: 2

Interface MAC Address       IP Address                              Product  DDP
                                                                    Category Ver
--------- ----------------- --------------------------------------- -------- ---
eth1/0/8  28-3B-82-7F-5A-08 10.90.90.90                             Switch   5
eth1/0/10 28-3B-82-AA-BB-CC 3FFE:22:33:44::55                       Switch   5

Switch#
```

Display Parameters

Interface	The interface on which the entry was received and learned.
MAC Address	The MAC address of the device.
IP Address	The IPv4/IPv6 address of the device.
Product Category	Identify the product type. **Switch** **AP**: Access point. **NC:** Network camera **VE:** Video encoder **NVR:** Network video recorder **NAS:** Network attached storage **SR:** Service router **WC:** Wireless controller **WS:** Wireless switch **WR:** Wireless router **EPOS**** **AAA-S:** AAA policy server **DS:** Digital signage **NP:** Network printer **CNTRLER:** Controller
DDP Ver	The DDP protocol version.

This example shows how to display the information of DDP neighbors in detail.

```
Switch#show ddp neighbors detail
Total Entries: 2

Interface: eth1/0/8
MAC Address: 28-3B-82-7F-5A-08
IP Address: 10.90.90.90
 Prefix Length: 24
 Model Name: DGS-3130-54TS
 DDP Version: 5
 Role: Client
 System Name: Switch-East1
 Product Category: Switch
 Firmware Version: 1.10.B024
 Hardware Version: A1
 Serial Number: DDLN7160002

Interface: eth1/0/10
MAC Address: 28-3B-82-AA-BB-CC
IP Address: 3FFE:22:33:44::55
 Prefix Length: 64
 Model Name: DGS-3130-54PS
 DDP Version: 5
 Role: Client
 System Name: Switch-East2
 Product Category: Switch
 Firmware Version: 1.10.T032
 Hardware Version: A1
 Serial Number: SG16114000021

Switch#
```

Display Parameters

Interface	The interface on which the entry was received and learned.
MAC Address	The MAC address of the device.
IP Address	The IPv4/IPv6 address of the device.
Prefix Length	The prefix length of the device.
Model Name	The model name of the device.
System Name	The name of the system.
Product Category	Identify the product type. This is carried in the DDP message.
Firmware Version	The firmware version of the device.
Hardware Version	The hardware version of the device.
DDP Version	The DDP protocol version.
Role	The role of the device. This can be the server or client.
Serial Number	The serial number of the device.

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 | *HOST-NAME***}**

Parameters

all	Specifies to clear all host entries.
HOST-NAME	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 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 the **ip domain lookup** 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)#
```

31-3 ip host

This command is used to configure the static mapping entry for the host name and the IP address in the host table. Use the **no** form of this command to remove the static host entry.

ip host *HOST-NAME* **{***IP-ADDRESS* | *IPV6-ADDRESS***}**

no ip host *HOST-NAME* **{***IP-ADDRESS* | *IPV6-ADDRESS***}**

Parameters

HOST-NAME	Specifies the host name of the equipment.
IP-ADDRESS	Specifies the IPv4 address of the equipment.
IPV6-ADDRESS	Specifies the IPv6 address of the equipment.

Default

None.

Command Mode

Global Configuration Mode.

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)#
```

31-4 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 {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

no ip name-server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [{***IP-ADDRESS2* **|** *IPV6-ADDRESS2***}]**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the domain name server.
IPV6-ADDRESS	Specifies the IPv6 address of the domain name server.
IP-ADDRESS2	Specifies multiple IP addresses, separated by spaces. Up to two servers can be specified.
IPV6-ADDRESS2	Specifies multiple IPv6 addresses, separated by spaces. Up to two 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)#
```

31-5 ip name-server timeout

This command is used to configure the timeout value for the name server. Use the **no** form of this command to revert to the default setting.

ip name-server timeout *SECONDS*

no ip name-server timeout

Parameters

SECONDS	Specifies the maximum time to wait for a response from a specified name server. This value must be between 1 and 60.

Default

By default, this value is 3 seconds.

Command Mode

Global Configuration Mode.

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)#
```

31-6 show hosts

This command is used to display the DNS configuration.

show hosts

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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:   1
 Number of Dynamic Entries:  0

 Host Name:          www.abc.com
 IP Address:         192.168.5.243
 TTL:                forever


Switch#
```

Display Parameters

TTL	The Time-To-Leave (TTL) value is displayed when the entry is a dynamic entry. The keyword “forever” is displayed when the entry is a static entry.

31-7 show ip name-server

This command is used to display the current DNS name servers.

show ip name-server

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the DNS name servers.

Example

This example shows how to display the DNS configuration when dynamic name server entries were received from the DHCP server.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:
 1.1.1.1
 1.1.1.2

Switch#
```

This example shows how to display the DNS configuration when no dynamic name server entry was received from the DHCP server.

```
Switch#show ip name-server

 Static name server:
 192.168.5.134
 5001:5::2

 Dynamic name server:

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 revert 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/Privileged EXEC 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#
```

32-3 snmp-server enable traps dos-prevention

This command is used to enable the sending of SNMP notifications for DoS attacking. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps dos-prevention

no snmp-server enable traps dos-prevention

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When DoS prevention is enabled, every five minutes, the Switch will log the event if any attack packet is received in this interval. Use this command to enable or disable the sending of SNMP notifications for such events.

Example

This example shows how to enable the sending of traps for DoS attacking.

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

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** form of this command to remove an ARP access-list.

arp access-list *NAME*

no arp access-list *NAME*

Parameters

NAME	Specifies the name of the ARP access-list to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

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 10.20.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#permit ip 10.30.0.0 255.255.0.0 mac any
Switch(config-arp-nacl)#
```

33-2 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

all	Specifies to clear dynamic ARP inspection statistics from all VLANs.
vlan *VLAN-ID*	Specifies the VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

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** form of this command to remove the specification.

ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

no ip arp inspection filter *ARP-ACL-NAME* **vlan** *VLAN-ID* **[, | -] [static]**

Parameters

ARP-ACL-NAME	Specifies the access control list name with a maximum of 32 characters.
vlan *VLAN-ID*	Specifies the VLAN associated with the ARP access list.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
static	(Optional) Specifies to drop the packet if the IP-to-Ethernet MAC binding pair is not permitted by the ARP ACL.

Default

None.

Command Mode

Global Configuration Mode.

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 and the **static** parameter is not specified, the packet will be further matched against the DHCP snooping binding entries. If the packet is denied due to the implicit deny and the **static** parameter is specified, the packet will be dropped.

Example

This example shows how to apply the ARP ACL static ARP list to VLAN 10 for DAI.

```
Switch#configure terminal
Switch(config)#ip arp inspection filter static-arp-list vlan 10
Switch(config)#
```

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 this command to revert to the default settings.

ip arp inspection limit {rate *VALUE* **[burst interval** *SECONDS***] | none}**

no ip arp inspection limit

Parameters

rate *VALUE*	Specifies the maximum number per second of the ARP packets that can be processed. The valid range is from 1 to 150.
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 this parameter is 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 eth1/0/10
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. Use the **no** form of this command to revert to the default setting.

ip arp inspection log-buffer entries *NUMBER*

no ip arp inspection log-buffer entries

Parameters

NUMBER	Specifies the buffer entry number. The maximum number is 1024.

Default

By default, this value is 32.

Command Mode

Global Configuration Mode.

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, 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 this 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 to be trusted for DAI.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
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 this command to remove specific additional check.

ip arp inspection validate [src-mac] [dst-mac] [ip]

no ip arp inspection validate [src-mac] [dst-mac] [ip]

Parameters

src-mac	(Optional) Specifies to check for ARP requests and response packets and the consistency of the source MAC address in the Ethernet header against the sender MAC address in the ARP payload.
dst-mac	(Optional) Specifies to check for ARP response packets and the consistency of the destination MAC address in the Ethernet header against the target MAC address in the ARP payload.
ip	(Optional) Specifies to check the ARP body for invalid and unexpected IP addresses. Specifies to check the validity of IP address in the ARP payload. The sender IP in both the ARP request and response and target IP in the ARP response are validated. Packets destined for the IP addresses 0.0.0.0, 255.255.255.255, and all IP multicast addresses are dropped. Sender IP addresses are checked in all ARP requests and responses, and target IP addresses are checked only in ARP responses.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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.

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 this command to disable dynamic ARP inspection for VLAN.

ip arp inspection vlan *VLAN-ID* **[, | -]**

no ip arp inspection vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the VLAN to enable or disable the ARP inspection function.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, ARP inspection is disabled on all VLANs.

Command Mode

Global Configuration Mode.

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 this command to revert to the default settings.

ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match {permit | all | none} | dhcp-bindings {permit | all | none}}**

no ip arp inspection vlan *VLAN-ID* **[, | -] logging {acl-match | dhcp-bindings}**

Parameters

VLAN-ID	Specifies the VLAN to enable or disable the logging control function.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
acl-match	Specifies the logging criteria for packets that are dropped or permitted based on ACL matches.
permit	Specifies logging when permitted by the configured ACL.
all	Specifies logging when permitted or denied by the configured ACL.
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.
permit	Specifies logging when permitted by DHCP bindings.
all	Specifies logging when permitted or denied by 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 this command to control the type of packets that are logged.

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

{permit | deny} ip {any | host *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

no {permit | deny} ip {any | host *SENDER-IP* **|** *SENDER-IP SENDER-IP-MASK***} mac {any | host** *SENDER-MAC* **|** *SENDER-MAC SENDER-MAC-MASK***}**

Parameters

ip	Specifies the source IP address.
any	Specifies to match any source IP address.
host *SENDER-IP*	Specifies to match a single source IP address.
SENDER-IP SENDER-IP-MASK	Specifies to match a group of source IP addresses by using a bitmap mask. The bit corresponding to bit value 1 will be checked. The input format is the same as IP address.
mac	Specifies the MAC address.
any	Specifies to match any source MAC address.
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 or range of ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
statistics	(Optional) Specifies the DAI statistics.
vlan *VLAN-ID*	(Optional) Specifies a VLAN or range of VLANs.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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     : Enabled
Destination MAC Validation: Disabled
IP Address Validation     : Disabled
VLAN State    ACL Match                        Static ACL
---- -------- -------------------------------- ----------
10   Disabled static-arp-list                  No
VLAN ACL Logging DHCP Logging
---- ----------- ------------
10   Deny        Deny

Switch#
```

Display Parameters

VLAN	The VLAN ID that enables ARP inspection.
State	The configuration state of ARP inspection. **Enabled:** ARP inspection is enabled. **Disabled:** 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 port 10.

```
Switch#show ip arp inspection interfaces eth1/0/10

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/10       trusted     None      1
Total Entries: 1

Switch#
```

This example shows how to display the trust state of interfaces on the Switch.

```
Switch#show ip arp inspection interfaces

Interface       Trust State Rate(pps) Burst Interval
--------------- ----------- --------- --------------
eth1/0/1        untrusted   15        1
eth1/0/2        untrusted   15        1
eth1/0/3        untrusted   15        1
eth1/0/4        untrusted   15        1
eth1/0/5        untrusted   15        1
eth1/0/6        untrusted   15        1
eth1/0/7        untrusted   15        1
eth1/0/8        untrusted   15        1
eth1/0/9        untrusted   15        1
eth1/0/10       trusted     None      1
eth1/0/11       untrusted   15        1
eth1/0/12       untrusted   15        1
eth1/0/13       untrusted   15        1
eth1/0/14       untrusted   15        1
eth1/0/15       untrusted   15        1
eth1/0/16       untrusted   15        1
eth1/0/17       untrusted   15        1
eth1/0/18       untrusted   15        1
eth1/0/19       untrusted   15        1
eth1/0/20       untrusted   15        1
eth1/0/21       untrusted   15        1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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/Privileged EXEC 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. Error Recovery Commands

34-1 errdisable recovery

This command is used to enable the error recovery for causes and to configure the recovery interval. Use the **no** form of this command to disable the auto-recovery option or to revert 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 *SECONDS***]**

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 L2PT guard.
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 and so on. When a port enters the error disabled state, the port is shutdown although the setting running the configuration remains in the no shutdown state.

There are two ways to recover an error disabled port. Administrators can use the **errdisable recovery cause** command to enable the auto-recovery of error ports disabled by each cause. Alternatively, administrators can manually recover the port by entering the **shutdown** command first and then the **no shutdown** command for the port.

Example

This example shows how to set the recovery timer to 200 seconds for port security violation.

```
Switch#configure terminal
Switch(config)#errdisable recovery cause psecure-violation interval 200
Switch(config)#
```

This example shows how to enable the auto-recovery option for port security violations.

```
Switch#configure terminal
Switch(config)#errdisable recovery cause psecure-violation
Switch(config)#
```

34-2 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/Privileged EXEC 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
--------------------------------------  ----------    -------------
Port Security                           disabled      300 seconds
Storm Control                           disabled      300 seconds
BPDU Attack Protection                  disabled      300 seconds
Dynamic ARP Inspection                  disabled      300 seconds
DHCP Snooping                           disabled      300 seconds
Loop Detection                          disabled      300 seconds
L2pt-guard                              disabled      300 seconds

Interfaces that will be recovered at the next timeout:

Interface    Errdisable Cause                       Time left(sec)
---------    --------------------------------------  --------------
eth1/0/7     BPDU Attack Protection                  infinite

Switch#
```

34-3 snmp-server enable traps errdisable

This command is used to enable the sending of SNMP notifications for the error disabled state. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps errdisable [asserted] [cleared] [notification-rate *TRAP-RATE***]**

no snmp-server enable traps errdisable [asserted] [cleared] [notification-rate]

Parameters

asserted	(Optional) Specifies to enable or disable the sending of SNMP notifications for entering the error disabled state.
cleared	(Optional) Specifies to enable or disable the sending of SNMP notifications for exiting the error disabled state.
notification-rate	(Optional) Specifies the number of traps per minute. The value is from 0 to 1000. If the number of packets exceeds the specified number, the exceeded packets will be dropped. 0 represents that there is no limitation for the sending of the SNMP traps for the error disabled state per minute.

Default

By default, this feature is disabled.

By default, the notification rate is 0.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If no parameter is specified, it will enable or disable the SNMP notifications for both entering and exiting the error disabled state. When only the **notification-rate** parameter is specified, the notification rate will be changed, and the state of sending notifications for the error disabled state will not be changed.

Example

This example shows how to enable the sending of the SNMP notification for the error disabled state.

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

35. Ethernet Ring Protection Switching (ERPS) Commands

35-1 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 ERPS instance.

Example

This example shows how to create an ERPS 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-erps-ring)#instance 1
Switch(config-erps-ring-instance)#description major-ring instance 1
Switch(config-erps-ring-instance)#
```

35-2 ethernet ring g8032

This command is used to create a G.8032 physical ring and enter the ERPS 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 ERPS 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-erps-ring)#
```

35-3 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-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#
```

35-4 tcn-propagation

This command is used to enable the propagation of topology change notifications from the sub-ERPS 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-erps-ring-profile)#tcn-propagation
Switch(config-erps-ring-profile)#
```

35-5 r-aps channel-vlan

This command is used to specify the APS channel VLAN for an ERPS instance. Use the **no** form of this 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 ERPS instance. The valid range is from 1 to 4094.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to assign the APS channel VLAN for an ERPS instance. The APS channel VLAN needs to be assigned before an ERPS instance can be set to operation state.

The specified APS channel VLAN needs to exist before the instance can be set to operation state.

Each ERPS 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 ERPS instance 1 as VLAN 2.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#r-aps channel-vlan 2
Switch(config-erps-ring-instance)#
```

35-6 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. Use the **no** form of this command to delete the set of VLAN IDs.

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 ERPS instance. The valid range from is 1 to 4094.

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

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the VLANs to be protected by the ERPS instance.

Example

This example shows how to configure the service protected VLAN as 100 to 200 for ERPS instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#r-aps channel-vlan 20
Switch(config-erps-ring-instance)#inclusion-list vlan-ids 100-200
Switch(config-erps-ring-instance)#
```

35-7 instance

This command is used to create an ERPS instance and enter the ERPS Instance Configuration Mode. Use the **no** form of this command to remove an ERPS instance.

instance *INSTANCE-ID*

no instance *INSTANCE-ID*

Parameters

INSTANCE-ID	Specifies the identifier of an ERPS instance. This value must be between 1 and 32.

Default

None.

Command Mode

ERPS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create an ERPS instance under a physical ring. Deploy multiple instances in the same physical ring topology provide the load balancing capability. The ID of ERPS instances in physical rings of the system are global significant.

Example

This example shows how to create an ERPS instance 1 in the physical ring named “major-ring”.

```
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#
```

35-8 level

This command is used to configure the ring MEL value of an ERPS instance. Use the **no** form of this command to revert to the default setting.

level *MEL-VALUE*

no level

Parameters

MEL-VALUE	Specifies the ring MEL value of the ERPS instance. The valid range is from 0 to 7.

Default

By default, this value is 1.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The configured ring MEL value of all ring nodes participating in the same ERPS instance should be the identical.

Example

This example shows how to configure the ring MEL value of ERPS instance 1 as 6.

```
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#level 6
Switch(config-erps-ring-instance)#
```

35-9 sub-ring

This command is used to specify the sub-ring default instance of a physical ring default instance. Use the **no** form of this command remove the sub-ring default instance of a physical ring default instance.

sub-ring *SUB-RING-NAME*

no sub-ring *SUB-RING-NAME*

Parameters

SUB-RING-NAME	Specifies the G8032 sub-ring's name.

Default

None.

Command Mode

ERPS 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-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#
```

35-10 sub-ring instance

This command is used to specify the sub-ring instance of a physical ring instance. Use the **no** form of this command to remove the sub-ring instance of a physical ring instance.

sub-ring instance *INSTANCE-ID*

no sub-ring instance *INSTANCE-ID*

Parameters

INSTANCE-ID	Specifies the identifier of an ERPS instance. The valid range is from 1 to 32.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure a sub-ring instance connected to another ring instance. This command is applied on the interconnection node.

Example

This example shows how to configure the physical ring named “ring2” instance 1 as a sub-ring of “ring1” instance 2

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#exit
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#instance 2
Switch(config-erps-ring-instance)#sub-ring instance 1
Switch(config-erps-ring-instance)#
```

35-11 profile

This command is used to associate an ERPS instance with a G.8032 profile. Use the **no** form of this 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 ERPS instance.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To change the profile association, deactivate the ERPS 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-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 interface eth1/0/2
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#profile campus
Switch(config-erps-ring-instance)#exit
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port0 interface eth1/0/3
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#instance 2
Switch(config-erps-ring-instance)#profile campus
Switch(config-erps-ring-instance)#
```

35-12 port0

This command is used to specify the first ring port of a physical ring. Use the **no** form of this command to remove the first ring port setting.

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

ERPS 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 port 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-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#
```

35-13 port1

This command is used to specify the second ring port of a physical ring. Use the **no** form of this command to remove the second ring port setting.

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 a sub-ring.

Default

None.

Command Mode

ERPS 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 a sub-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-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring1
Switch(config-erps-ring)#sub-ring ring2
Switch(config-erps-ring)#exit
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#port1 none
Switch(config-erps-ring)#
```

35-14 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 this 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-erps-ring-profile)#no revertive
Switch(config-erps-ring-profile)#
```

35-15 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 | neighbor]

no rpl

Parameters

port0	Specifies port 0 as the RPL port.
port1	Specifies port 1 as the RPL port.
owner	(Optional) Specifies the ring node as the RPL owner node for the configured instance.
neighbor	(Optional) Specifies the ring node as the RPL neighbor node for the configured instance.

Default

None.

Command Mode

ERPS 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 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 ERPS instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#port0 interface eth1/0/1
Switch(config-erps-ring)#port1 interface eth1/0/2
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#rpl port0 owner
Switch(config-erps-ring-instance)#
```

35-16 show ethernet ring g8032

This command is used to display information of the ERPS instance.

show ethernet ring g8032 status [*RING-NAME***] [instance [***INSTANCE-ID***]]**

show ethernet ring g8032 brief [*RING-NAME***] [instance [***INSTANCE-ID***]]**

show ethernet ring g8032 profile [*PROFILE-NAME***]**

Parameters

RING-NAME	(Optional) Specifies to display information of the specified ERPS physical ring.
PROFILE-NAME	(Optional) Specifies to display information of the specified ERPS profile.
INSTANCE-ID	(Optional) Specifies to display information of the specified ERPS instance.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display information of the ERPS.

Example

This example shows how to display detailed information of ERPS.

```
Switch#show ethernet ring g8032 status

 ERPS Version: G.8032v2
 ----------------------------
 Ethernet Ring ring1
 Admin Port0: eth1/0/1
 Admin Port1: eth1/0/2
 Ring Type: Major ring
 Ring ID: 1
 ----------------------------
 Instance  : 1
 Instance Status: Idle
 R-APS Channel : 2,Protected VLANs:3
 Port0: eth1/0/1, Blocking
 Port1: eth1/0/2, Forwarding
 Profile: 1
 Description :
 Guard Timer: 500 milliseconds
 Hold-off Timer: 0 milliseconds
 WTR Timer: 1 minutes
 Revertive
 MEL: 1
 RPL Role: Owner
 RPL Port: Port0
 Sub Ring Instance: none


Switch#
```

This example shows how to display detailed information of the ERPS physical ring “ring1”.

```
Switch#show ethernet ring g8032 status ring1

 Ethernet Ring ring1
 Admin Port0: eth1/0/1
 Admin Port1: eth1/0/2
 Ring Type: Major ring
 Ring ID: 1
 ----------------------------
 Instance  : 1
 Instance Status: Idle
 R-APS Channel : 2,Protected VLANs:3
 Port0: eth1/0/1, Blocking
 Port1: eth1/0/2, Forwarding
 Profile: 1
 Description :
 Guard Timer: 500 milliseconds
 Hold-off Timer: 0 milliseconds
 WTR Timer: 1 minutes
 Revertive
 MEL: 1
 RPL Role: Owner
 RPL Port: Port0
 Sub Ring Instance: none


Switch#
```

This example shows how to display detailed information of the ERPS profile “file1”.

```
Switch#show ethernet ring g8032 profile file1

Ethernet Ring Profile file1
Guard Timer: 500 milliseconds
Hold-off Timer: 0 milliseconds
WTR Timer: 5 minutes

Switch#
```

This example shows how to display detailed information of the ERPS physical ring's major-ring instance 1:

```
Switch#show ethernet ring g8032 status major-ring instance 1

Instance  : 1
 Instance Status: Deactivated
 R-APS Channel : 0,Protected VLANs:
 Port0: eth1/0/1, Forwarding
 Port1: eth1/0/2, Forwarding
 Profile: file1
 Description :
 Guard Timer: 500 milliseconds
 Hold-off Timer: 0 milliseconds
 WTR Timer: 5 minutes
 Revertive
 MEL: 1
 RPL Role: None
 RPL Port: -
 Sub Ring Instance: none

Switch#
```

This example shows how to display brief information of the ERPS physical ring "ring1"

```
Switch#show ethernet ring g8032 brief ring1

ERPS Version : G.8032v2
Ring                            InstID  Status      Port-State
-----                            ----    -----       -------
ring1                            1       Deactivated p0:eth1/0/3,Forwarding
                                                     p1:eth1/0/2,Forwarding

Switch#
```

This example shows how to display brief information of the ERPS physical ring "ring1" instance 1

```
Switch#show ethernet ring g8032 brief ring1 instance 1

ERPS Version : G.8032v2
Ring                            InstID  Status      Port-State
-----                            ----    -----       -------
ring1                            1       Deactivated p0:eth1/0/3,Forwarding
                                                     p1:eth1/0/2,Forwarding

Switch#
```

Display Parameters

MEL	The ring MEL value of the ERPS instance.
R-APS Channel	The APS channel VLAN of the ERPS instance.
Protected VLANs	Service protected VLANs of the ERPS instance.
Profile	The profile associated with the ERPS instance.
Guard Timer	The time value for the guard timer of the profile.
Hold-Off Timer	The time value for hold-off timer of the profile.
WTR Timer	The time value for the WTR timer of the profile.

TC Propagation State	TC is propagated or not propagated in the ring instance.
Revertive / Non-revertive	Ring instances are operated revertively or non-revertively in the profile.
Instance Status	The current ring node status of the ERPS instance. (Deactivated / Init / Idle / Protection / force / manual / pending)
RPL Role	The current config/running config ring node role of the ERPS instance. (Owner / Neighbor / None)
Port0 / Port1	The current config/running config ring port role. (Interface_id / virtual_channel)
RPL Port	The current config/running RPL. (Port0 / Port1 / None)
Ring port0/port1 state	The state for ring ports of the ERPS instance. (Forwarding / Blocking / SF / SF blocked)
RingType	Indicates either Major ring or Sub ring.

35-17 activate

This command is used to activate an ERPS instance. Use the **no** form of this command to deactivate an ERPS instance.

activate

no activate

Parameters

None.

Default

By default, this option is disabled.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to activate an ERPS instance. The ring ports, and APS channel must be configured first before an ERPS instance can be activated.

In addition to these configurations, the configuration of service protected VLANs and RPL related settings are fundamental for operation of an ERPS 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-erps-ring)#instance 1
Switch(config-erps-ring-instance)#profile campus
Switch(config-erps-ring-instance)#activate
Switch(config-erps-ring-instance)#
```

35-18 timer

This command is used to configure timers for an ERPS profile. Use the **no** form of this command to revert to the default setting.

timer {guard *MILLI-SECONDS* **| hold-off** *SECONDS* **| wtr** *MINUTES***}**

no timer [guard | hold-off | wtr]

Parameters

guard *MILLI-SECONDS*	Specifies the guard timer in milliseconds. The valid range is from 10 to 2000. The value should be multiples of 10.
hold-off *SECONDS*	Specifies the hold-off timer in seconds. The valid range is from 0 to 10.
wtr *MINUTES*	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 ERPS instances associated with the profile. Use the **no** form of this command to revert to the default setting. If no parameter is specified in the **no** form of this command, all timers will be reset.

Example

This example shows how to configure the guard timer to 700 milliseconds, hold-off timer to 1 second, and WTR timer to 1 minute for profile “campus”.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 profile campus
Switch(config-erps-ring-profile)#timer guard 700
Switch(config-erps-ring-profile)#timer hold-off 1
Switch(config-erps-ring-profile)#timer wtr 1
Switch(config-erps-ring-profile)#
```

35-19 ring_id

This command is used to specify the ring ID of a physical ring. Use the **no** form of this command to remove the configuration.

ring_id *RING_ID*

no ring_id

Parameters

RING-ID	Specifies the identifier of a physical ring. The valid range is from 1 to 239.

Default

None.

Command Mode

ERPS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the ring ID of a physical ring. A different ring ID, in ERPSv2, must be assigned to each physical ring.

This command is used in ERPSv2 only.

Example

This example shows how to configure the ring value 2 of the G8032 ring “ring2”.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#ring_id 2
Switch(config-erps-ring)#
```

35-20 ring_type

This command is used to specify the ring type of a physical ring. Use the **no** form of this command to revert to the default setting.

ring_type {major-ring | sub-ring}

no ring_type

Parameters

major-ring	Specifies an ERPS ring as a major-ring.
sub-ring	Specifies an ERPS ring as a sub-ring.

Default

By default, the ERPS ring is a major-ring.

Command Mode

ERPS Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to indicate that the ring is an open or a closed ring.

This command is used in ERPSv2 only.

Example

This example shows how to configure the interconnect node “ring2 ”as a sub-ring:

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 ring2
Switch(config-erps-ring)#ring_type sub-ring
Switch(config-erps-ring)#
```

35-21 erps force switch ring_port

This command is used to block an ERPS instance port.

erps force switch ring_port {port0 | port1}

Parameters

port0	Specifies that port0 will be blocked.
port1	Specifies that port1 will be blocked.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command forcibly blocks an instance port immediately after force is configured, irrespective of whether link failures have occurred. This command is used in ERPSv2 only.

Example

This example shows how to force the major ring, instance 1, port0 into blocking.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps force switch ring_port port0
Switch(config-erps-ring-instance)#
```

35-22 erps manual switch ring_port

This command is used to block an ERPS instance port.

erps manual switch ring_port {port0 | port1}

Parameters

port0	Specifies to manually block ERPS instance port0.
port1	Specifies to manually block ERPS instance port1.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command forcibly blocks a port on which MS is configured when link failures and FS conditions are absent.

This command is used in ERPSv2 only.

Example

This example shows how to manually block the major-ring instance 1 port0.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps manual switch ring_port port0
Switch(config-erps-ring-instance)#
```

35-23 clear

This command is used to clear the local active administrative command.

clear

Parameters

None.

Default

None.

Command Mode

ERPS Instance Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A **clear** command will remove the effects of the **force** and **manual** commands.

The **clear** command also provides the following functions:

- Triggers revertive switching before the WTR or WTB timer expires in the case of revertive operations.
- Triggers revertive switching in the case of non-revertive operations.

This command is used in ERPSv2 only.

Example

This example shows how to clear the local manual command on the major-ring instance 1.

```
Switch#configure terminal
Switch(config)#ethernet ring g8032 major-ring
Switch(config-erps-ring)#instance 1
Switch(config-erps-ring-instance)#erps manual switch ring_port port0
Switch(config-erps-ring-instance)#clear
Switch(config-erps-ring-instance)#
```

35-24 erps version

This command is used to configure the ERPS version. Use the **no** form of this command to revert to the default setting.

erps version {G.8032v1 | G.8032v2}

no erps version

Parameters

G.8032v1	Specifies to use the G.8032v1 ERPS version.
G.8032v2	Specifies to use the G.8032v2 ERPS version.

Default

By default, G.8032v2 is used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

G.8032v2 fully provides the following enhanced functions:

- Supports multi-instance in a physical ring.
- Supports operation commands: manual, force, and clear.
- Supports the configuration of the sending of a R-APS PDU destination address with the physical ring's ring ID.

Before specifying G.8032v1 for a G.8032v2 device, changing the ERPS version will lead to the restart of the running protocol.

If Ethernet ring nodes running ITU-T G.8032v1 and ITU-T G.8032v2 co-exist on an Ethernet ring, the following configurations should be met on the G.8032v2 device:

- All physical ring IDs have the default value of 1.
- Interconnection node's major ring and sub-ring instances must have different R-APS VIDs.
- Manual switch or force switch commands not exist.
- Physical rings have only one instance.

Example

This example shows how to set the ERPS version.

```
Switch#configure terminal
Switch(config)#erps version G.8032v1
Switch(config)#
```

36. File System Commands

36-1 cd

This command is used to change the current directory.

cd [*DIRECTORY-URL***]**

Parameters

DIRECTORY-URL	(Optional) Specifies the URL of the directory. If this parameter is 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

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If the URL is not specified, the current directory is not changed.

Example

This example shows how to change the current directory to the directory “d” on file system.

```
Switch#dir

Directory of /c:
1   d--             0 Jan 01 2019 03:12:49  d
2   -rw      14993776 Jan 01 2019 00:18:42  runtime.had
3   -rw      14991008 Jan 01 2019 00:26:02  Run-1.00.029.had
4   -rw          1802 Jan 01 2019 00:02:18  config.cfg
5   -rw      14887648 Jan 01 2019 04:56:22  Run-1.01.004.had
6   d--             0 Jan 01 2019 00:00:10  system

62283264 bytes total (16477184 bytes free)

Switch#cd d
Switch#
```

This example shows how to display the current directory.

```
Switch#cd
Current directory is /c:
Switch#
```

36-2 delete

This command is used to delete a file.

delete *FILE-URL*

Parameters

FILE-URL	Specifies the name of the file to be deleted.

Default

None.

Command Mode

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#
```

36-3 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

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If URL is not specified, the current directory is used. By default, the current directory 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 Jan 01 2019 00:00:10  c:

0 bytes total (0 bytes free)

Switch#
```

36-4 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#
```

36-5 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 “config.cfg”.

```
Switch#more config.cfg


!----------------------------------------------------------------------------
!                  DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                                Configuration
!
!                             Firmware: Build 1.01.004
!           Copyright(C) 2022 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
!
ip http server
ip http service-port 80
ip http timeout-policy idle 180
no ip http secure-server
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

36-6 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#
```

36-7 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#
```

36-8 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.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the information of the storage media available on the system. If no parameter is specified, all units are displayed.

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       59 MB     FFS

Switch#
```

Display Parameters

Media-Type	**Flash:** This represents the storage in the Switch.

37. Filter Database (FDB) Commands

37-1 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

Use this command to only clear dynamic MAC address entries. Only the dynamic unicast address entry will be cleared.

Example

This example shows how to remove the MAC address 00:08:00:70:00:07 from the dynamic MAC address table.

```
Switch#clear mac-address-table dynamic address 00:08:00:70:00:07
Switch#
```

37-2 mac-address-table aging-time

This command is used to configure the MAC address table ageing time. Use the **no** form of this command to revert to the default setting.

mac-address-table aging-time *SECONDS*

no mac-address-table aging-time

Parameters

SECONDS	Specifies the aging time in seconds. The valid range is 0 or 10 to 1000000 seconds. Setting the aging time to 0 will disable the MAC address table aging out function.

Default

By default, this value is 300 seconds.

Command Mode

Global Configuration Mode.

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)#
```

37-3 mac-address-table aging destination-hit

This command is used to enable the destination MAC address triggered update function. Use the **no** form of this 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)#
```

37-4 mac-address-table learning

This command is used to enable MAC address learning on the physical port or VLAN. Use the **no** form of this command to disable learning.

mac-address-table learning interface {vlan *VLAN-ID* **[, | -] |** *INTERFACE-ID* **[, | -]}**

no mac-address-table learning interface {vlan *VLAN-ID* **[, | -] |** *INTERFACE-ID* **[, | -]}**

Parameters

vlan *VLAN-ID*	Specifies the VLAN ID to be configured.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
INTERFACE-ID	(Optional) Specifies the physical port interface to be configured.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this commands to enable or disable MAC address learning on a physical port or VLAN.

The behavior of MAC addresses learning on VLAN interfaces:

By default, MAC address learning is always enabled on all VLANs on the Switch when VLAN is created. MAC address learning will be recovered to the default value when a VLAN is deleted.

MAC address learning only can be configured on the existed VLAN.

Disabling MAC address learning on a VLAN will cause all ports belong to this VLAN stop the MAC address learning.

Disabling MAC address learning on the voice or surveillance VLAN, the function will work abnormally based on MAC address learning.

Disabling MAC address learning on a VLAN will cause asymmetric VLAN work abnormally on the related VLAN.

Disabling MAC address learning on a private VLAN will cause related private VLAN work abnormally.

RSPAN VLAN has the higher precedence, and MAC address learning is always disabled on the RSPAN VLAN. If RSPAN VLAN is deleted, the configured MAC address learning state takes effect.

The MAC address learning for the secure modules such as Port Security, 802.1x, MAC-based Access Control, Web-based Access Control and IMPB has the higher precedence. If MAC address learning on a VLAN that includes a secure port is disabled, MAC address learning is not disabled on the VLAN. If all the secure ports on the VLAN are disabled, the configured MAC address learning state takes effect.

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)#
```

37-5 mac-address-table notification change

This command is used to enable or configure the MAC address notification function. Use the **no** form of this command to disable the function or set the optional configuration to default.

mac-address-table notification change [interval *SECONDS* **| history-size** *VALUE* **| trap-type {with-vlanid | without-vlanid}]**

no mac-address-table notification change [interval | history-size | trap-type]

Parameters

interval *SECONDS*	(Optional) Specifies the interval of sending the MAC address trap message. The range is 1 to 2147483647 and the default value is 1 second.
history-size *VALUE*	(Optional) Specifies the maximum number of the entries in the MAC history notification table. The range is 0 to 500 and the default value is 1 entry.
trap-type	(Optional) Specifies the trap information to include VLAN ID or not.
with-vlanid	Specifies the trap information to include VLAN ID.
without-vlanid	Specifies the trap information to exclude VLAN ID.

Default

MAC address notification is disabled.

The default trap interval is 1 second.

The default number of entries in the history table is 1.

The default trap type is without-vlanid.

Command Mode

Global Configuration Mode.

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)#
```

37-6 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. The 01-80-C2-XX-XX-XX range are for reserved MAC addresses. The 01-00-5E-XX-XX-XX range are reserved for IPv4 multicast MAC addresses. The 33-33-XX-XX-XX range are reserved for IPv6 multicast MAC addresses.
vlan *VLAN-ID*	Specifies the VLAN of the entry. The range is 1 to 4094.
interface *INTERFACE-ID*	Specifies the forwarding ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
drop	Specifies to drop the frames that are sent by or sent to the specified MAC address on the specified VLAN.
all	Specifies to remove all static MAC address entries.

Default

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 **drop** parameter can only be specified for a unicast MAC address entry.

Example

This example shows how to add the static address C2:F3:22:0A:12:F4 to the MAC address table. It also specifies that when any packet received on VLAN 4 that has a destination MAC address of C2:F3:22:0A:12:F4 will be forwarded to port 1.

```
Switch#configure terminal
Switch(config)#mac-address-table static C2:F3:22:0A:12:F4 vlan 4 interface eth1/0/1
Switch(config)#
```

37-7 multicast filtering-mode

This command is used to configure the handling method for multicast packets for an interface. Use the **no** form of this command to revert to the default setting.

multicast filtering-mode {forward-all | forward-unregistered | filter-unregistered}

no multicast filtering-mode

Parameters

forward-all	Specifies to flood all multicast packets based on the VLAN domain.
forward-unregistered	Specifies to forward registered multicast packets based on the forwarding table and flood all unregistered multicast packets based on the VLAN domain.
filter-unregistered	Specifies to forward registered packets based on the forwarding table and filter all unregistered multicast packets.

Default

By default, the **forward-unregistered** option is enabled.

Command Mode

VLAN Configuration Mode.

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)#
```

37-8 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If the **interface** parameter is specified, the unicast entry that has the forwarding interface matches the specified interface will be displayed.

Example

This example shows how to display all the MAC address table entries for the MAC address 00-23-7D-BC-08-44.

```
Switch#show mac-address-table address 00-23-7D-BC-08-44

VLAN  MAC Address        Type        Ports
----  -----------------  ----------  -------------------------
1     00-23-7D-BC-08-44  Dynamic     eth1/0/5

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     F0-7D-68-34-00-10  Static      CPU

Total Entries: 1

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     00-23-7D-BC-08-44  Dynamic     eth1/0/5
1     00-23-7D-BC-2E-18  Dynamic     eth1/0/1
1     00-FF-47-77-70-B8  Dynamic     eth1/0/5
1     10-BF-48-D6-E2-E2  Dynamic     eth1/0/5
1     24-24-0E-E5-96-DE  Dynamic     eth1/0/5
1     40-B8-37-B1-06-9A  Dynamic     eth1/0/5
1     5C-33-8E-43-B3-68  Dynamic     eth1/0/5
1     CC-B2-55-8B-27-79  Dynamic     eth1/0/5
1     F0-7D-68-34-00-10  Static      CPU

Total Entries: 9

Switch#
```

37-9 show mac-address-table aging-time

This command is used to display the aging time of the MAC address table.

show mac-address-table aging-time

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the aging time of the MAC address table.

Example

This example shows how to display the aging time of the MAC address table.

```
Switch#show mac-address-table aging-time

Aging Time is 300 seconds

Switch#
```

37-10 show mac-address-table learning

This command is used to display the MAC-address learning state.

show mac-address-table learning interface [vlan [*VLAN-ID* **[, | -]] | *INTERFACE-ID* [, | -]]**

Parameters

VLAN-ID	(Optional) Specifies the VLAN ID to be displayed. If not specified, all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
INTERFACE-ID	(Optional) Specifies the interface to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no parameter is specified, all physical ports will be displayed.

Example

This example shows how to display the MAC address learning status on ports 1 to 10.

```
Switch#show mac-address-table learning interface eth1/0/1-10

Port                        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#
```

37-11 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no parameter is specified, the global configuration will be displayed. Use the **interface** parameter to display information of all interfaces. Use the **interface** *INTERFACE-ID* parameter to display information of the specified interface.

Example

This example shows how to display the MAC address notification change configuration on all interfaces.

```
Switch#show mac-address-table notification change interface

Interface                Added Trap       Removed Trap
-----------------------  --------------   --------------

eth1/0/1                 Disabled         Disabled
eth1/0/2                 Disabled         Disabled
eth1/0/3                 Disabled         Disabled
eth1/0/4                 Disabled         Disabled
eth1/0/5                 Disabled         Disabled
eth1/0/6                 Disabled         Disabled
eth1/0/7                 Disabled         Disabled
eth1/0/8                 Disabled         Disabled
eth1/0/9                 Disabled         Disabled
eth1/0/10                Disabled         Disabled
eth1/0/11                Disabled         Disabled
eth1/0/12                Disabled         Disabled
eth1/0/13                Disabled         Disabled
eth1/0/14                Disabled         Disabled
eth1/0/15                Disabled         Disabled
eth1/0/16                Disabled         Disabled
eth1/0/17                Disabled         Disabled
eth1/0/18                Disabled         Disabled
eth1/0/19                Disabled         Disabled
eth1/0/20                Disabled         Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

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
Trap Type: Without VID

Switch#
```

This example shows how to display the MAC address notification history.

```
Switch#show mac-address-table notification change history

History Index: 1
Operation:ADD Vlan: 1 MAC Address: 00-f8-d0-12-34-56 eth1/0/1
History Index: 2
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-01 eth1/0/1
History Index: 3
Operation:DEL Vlan: 1 MAC Address: 00-f8-d0-00-00-02 eth1/0/1

Switch#
```

37-12 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 *INTERFACE-ID***]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the VLAN to display.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the filtering mode for handling multicast packets that are received on an interface.

Example

This example shows how to display the multicast filtering mode configuration for all VLANs.

```
Switch#show multicast filtering-mode

Interface                       Layer 2 Multicast Filtering Mode
------------------------------  --------------------------------
default                         forward-unregistered

Total Entries: 1

Switch#
```

37-13 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 this command to disable the sending of SNMP MAC notification traps.

snmp-server enable traps mac-notification change

no snmp-server enable traps mac-notification change

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of SNMP MAC notification traps.

Example

This example shows how to enable the sending of SNMP MAC notification traps.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps mac-notification change
Switch(config)#
```

37-14 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 this command to revert to the default setting.

snmp trap mac-notification change {added | removed}

no snmp trap mac-notification change{added | removed}

Parameters

added	Specifies to enable the MAC change notification when a MAC address is added on the interface.
removed	Specifies to enable the MAC change notification when a MAC address is removed from the interface.

Default

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 port 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#snmp trap mac-notification change added
Switch(config-if)#
```

38. Filter NetBIOS Commands

38-1 deny netbios

This command is used to deny NetBIOS packets on the specified interface. Use the **no** form of this command to revert to the default setting.

deny netbios

no deny netbios

Parameters

None.

Default

By default, NetBIOS packets are permitted.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Using this command to deny or permit NetBIOS packets on physical ports.

Example

This example shows how to deny NetBIOS packets on port 1.

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

38-2 deny extensive-netbios

This command is used to deny NetBIOS packets over 802.3 frame on the specified interface. Use the **no** form of this command to revert to the default setting.

deny extensive-netbios

no deny extensive-netbios

Parameters

None.

Default

By default, NetBIOS packets over 802.3 frame are permitted.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical ports. Using this command to deny or permit NetBIOS packets over 802.3 frame.

Example

This example shows how to deny NetBIOS packets over 802.3 frame on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#deny extensive-netbios
Switch(config-if)#
```

39. GARP VLAN Registration Protocol (GVRP) Commands

39-1 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 to be configured.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

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#
```

39-2 gvrp global

This command is used to enable the GVRP function globally. Use the **no** form of this 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)#
```

39-3 gvrp enable

This command is used to enable the GVRP function on a port. Use the **no** form of this 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 port 1.

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

39-4 gvrp advertise

This command is used to specify the VLAN that are allowed to be advertised by the GVRP protocol. Use the **no** form of this 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	Specified the VLAN ID 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 separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp advertise 1000
Switch(config-if)#
```

39-5 gvrp vlan create

This command is used to enable dynamic VLAN creation. Use the **no** form of this 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)#
```

39-6 gvrp forbidden

This command is used to specify a port as being a forbidden member of the specified VLAN. Use the **no** form of this 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	Specified the forbidden VLAN list. If the **add** or **remove** parameter 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 separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

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 port 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)#
```

39-7 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	(Optional) 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#gvrp timer leave-all 500
Switch(config-if)#
```

39-8 gvrp nni-bpdu-address

This command is used to configure the GVRP BPDU address in the service provider site. Use the **no** form of this command to revert 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

By default, 802.1d GVRP address is used.

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)#
```

39-9 show gvrp configuration

This command is used to display the GVRP settings.

show gvrp configuration [interface [*INTERFACE-ID* **[, | -]]]**

Parameters

interface	(Optional) Specifies to display the GVRP interface configuration. If the interface ID is not specified, all interfaces are displayed.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command only displays GVRP related configurations. If no parameter is specified, the GVRP global configuration is displayed.

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 ports 5 to 6.

```
Switch#show gvrp configuration interface eth1/0/5-6

ethernet 1/0/5
GVRP Status     : Enabled
Join Time       : 20 centiseconds
Leave Time      : 60 centiseconds
Leave-All Time  : 1000 centiseconds
Advertise VLAN  : 1-4094
Forbidden VLAN  : 3-5

ethernet 1/0/6
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#
```

39-10 show gvrp statistics

This command is used to display the statistics for a GVRP port.

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 GVRP interfaces statistics on ports 5 to 6.

```
Switch#show gvrp statistics interface eth1/0/5-6

 Interface      JoinEmpty  JoinIn     LeaveEmpty LeaveIn   LeaveAll   Empty
 ------------------------------------------------------------------------------
 eth1/0/5    RX 0          0          0          0         0          0
             TX 4294967296 4294967296 4294967296 42949672964294967296 4294967296
 eth1/0/6    RX 0          0          0          0         0          0
             TX 0          0          0          0         0          0

Switch#
```

40. Gratuitous ARP Commands

40-1 ip arp gratuitous

This command is used to enable the learning of gratuitous ARP packets in the ARP cache table. Use the **no** form of this command to disable ARP control.

ip arp gratuitous

no ip arp gratuitous

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

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)#
```

40-2 ip gratuitous-arps

This command is used to enable the transmission of gratuitous ARP request packets. Use the **no** form of this command to disable the transmission.

ip gratuitous-arps [dad-reply]

no ip gratuitous-arps [dad-reply]

Parameters

dad-reply	(Optional) Specifies control whether the system will reply with another gratuitous ARP request packet with the broadcast DA, when receiving a gratuitous ARP request packet and detecting the duplicate IP address.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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)#
```

40-3 arp gratuitous-send interval

This command is used to set the interval for regularly sending of gratuitous ARP request messages on the interface. Use the **no** form of this command to disable this function on the interface.

arp gratuitous-send interval *SECONDS*

no arp gratuitous-send interval

Parameters

SECONDS	Specifies the time interval to send the gratuitous ARP request message. The value is from 0 to 3600. 0 represents that this option is disabled.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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)#
```

40-4 snmp-server enable traps gratuitous-arp

This command is used to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected. Use the **no** form of this command to disable the function.

snmp-server enable traps gratuitous-arp

no snmp-server enable traps gratuitous-arp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

Example

This example shows how to enable the sending of SNMP notifications for gratuitous ARP duplicate IP detected.

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

41. Interface Commands

41-1 clear counters

This command is used to clear counters for the specified interfaces.

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

Parameters

all	Specifies to clear counters for all interfaces.
interface *INTERFACE-ID*	Specifies the interfaces to be configured. The interfaces can be physical ports, port-channels or Layer 2 VLAN interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear counters for all interfaces or the specified interface(s).

Example

This example shows how to clear the counters on port 1.

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

41-2 description

This command is used to add a description to an interface. Use the **no** form of this command to delete the description.

description *STRING*

no description

Parameters

STRING	Specifies a description for an interface with a maximum of 64 characters.

Default

None.

Command Mode

Interface Configuration Mode.

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 port 10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#description Physical Port 10
Switch(config-if)#
```

41-3 interface

This command is used to enter the Interface Configuration Mode for a single interface. Use the **no** form of this command to remove an interface.

interface *INTERFACE-ID*

no interface *INTERFACE-ID*

Parameters

INTERFACE-ID	Specifies the ID of the interface. The interface ID is formed by interface type and interface number 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 physical Ethernet switch port with all different media.
- **L2vlan** - Specifies the IEEE 802.1Q Layer 2 Virtual LAN interface.
- **Loopback** - Specifies the software only interface which always stays in the up status.
- **mgmt** - Specifies the Ethernet interface used for the out-of-band management port. **(DGS-1520-28 and DGS-1520-52 Only)**
- **Null** - Specifies the null interface.
- **Port-channel** - Specifies the aggregated port-channel interface.
- **Vlan** - Specifies the VLAN interface.

The format of the interface number is dependent on the interface type.

For physical port interfaces, the user cannot enter the interface if the Switch port does not exist. The physical port interface cannot be removed by the **no** command.

Use the **interface Vlan** command to create Layer 3 interfaces. Use the **vlan** command in the Global Configuration Mode to create a VLAN before creating Layer 3 interfaces. Use the **no interface Vlan** command to remove a Layer 3 interface.

The port-channel interface is automatically created when the **channel-group** command is configured for the physical port interface. A port-channel interface will be automatically removed when no physical port interface has the **channel-group** command configured for it. Use the **no interface Port-channel** command to remove a port-channel.

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.

L2vlan interface is only used to add descriptions to existed L2 VLANs. The **interface l2vlan** command does not create new interface, neither will the **no** form of this command removed any existing interface.

Example

This example shows how to enter the Interface Configuration Mode for port 5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#
```

This example shows how to enter the interface configuration mode on VLAN 100.

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

This example shows how to enter the interface configuration mode on port-channel 3.

```
Switch#configure terminal
Switch(config)#interface port-channel3
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)#
```

41-4 interface range

This command is used to enter the Interface Range Configuration Mode for multiple interfaces.

interface range *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the ID of the interface. The interface ID is formed by interface type and interface number with no spaces in between.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enter the Interface Range Configuration Mode for the specified range of interfaces. All Commands configured in the Interface Range Configuration Mode apply to all interfaces specified in the range.

Example

This example shows how to enter the Interface Range Configuration Mode for ports 1 to 5 and port 8.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-5,1/0/8
Switch(config-if-range)#
```

41-5 show counters

This command is used to display interface information.

show counters [interface *INTERFACE-ID***]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies that the interface can be a physical port, port channel or Layer 2 VLAN interfaces. If no interface is specified, counters of all interfaces will be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the statistic counters for an interface.

A particular rate statistics of a port-channel is the sum of all physical member port interface rate for that port-channel. For example, physical ports 1 to 4 belong to the same port-channel, the RX rate (packets per second) of each port is 100, 200, 200,100. As a result, the CRC error packets of the port-channel is 600 packets per second.

The following items provide detail information about the display parameters of this command:

- **max-rcv-frame-size:** The maximum Ethernet frame size which is defined in **Jumbo Frame Commands**. The range is from 64 to 12288 bytes.

Example

This example shows how to display the counters on port 1.

```
Switch#show counters interface eth1/0/1

eth1/0/1 counters
rxHCTotalPkts                      : 45340
txHCTotalPkts                      : 11516
rxHCUnicastPkts                    : 18220
txHCUnicastPkts                    : 11516
rxHCMulticastPkts                  : 24994
txHCMulticastPkts                  : 0
rxHCBroadcastPkts                  : 2126
txHCBroadcastPkts                  : 0
rxHCOctets                         : 5876961
txHCOctets                         : 5111397
rxHCPkt64Octets                    : 31884
rxHCPkt65to127Octets               : 5800
rxHCPkt128to255Octets              : 1005
rxHCPkt256to511Octets              : 3208
rxHCPkt512to1023Octets             : 3443
rxHCPkt1024to1518Octets            : 0
rxHCPkt1519to1522Octets            : 0
rxHCPkt1519to2047Octets            : 0
rxHCPkt2048to4095Octets            : 0
rxHCPkt4096to9216Octets            : 0
rxHCPkt9217to16383Octets           : 0
txHCPkt64Octets                    : 183
txHCPkt65to127Octets               : 5054
txHCPkt128to255Octets              : 1082
txHCPkt256to511Octets              : 2481
txHCPkt512to1023Octets             : 560
txHCPkt1024to1518Octets            : 2156
txHCPkt1519to1522Octets            : 0
txHCPkt1519to2047Octets            : 0
txHCPkt2048to4095Octets            : 0
txHCPkt4096to9216Octets            : 0
txHCPkt9217to16383Octets           : 0

rxCRCAlignErrors                   : 0
rxUndersizedPkts                   : 0
rxOversizedPkts                    : 0
rxFragmentPkts                     : 0
rxJabbers                          : 0
rxSymbolErrors                     : 0
rxBufferFullDropPkts               : 0
rxACLDropPkts                      : 0
rxMulticastDropPkts                : 0
rxVLANIngressCheckDropPkts         : 0
rxIpv6DropPkts                     : 0
rxSTPDropPkts                      : 0
rxStormAndTableDropPkts            : 0
rxMTUDropPkts                      : 0

txCollisions                       : 0
ifInErrors                         : 0
ifOutErrors                        : 0
```

```
ifInDiscards                        : 24616
ifOutDiscards                       : 0
ifInUnknownProtos                   : 0
txDelayExceededDiscards             : 0
txCRC                               : 0
txSTPDropPkts                       : 0
txHOLDropPkts                       : 0

dot3StatsAlignmentErrors            : 0
dot3StatsFCSErrors                  : 0
dot3StatsSingleColFrames            : 0
dot3StatsMultiColFrames             : 0
dot3StatsSQETestErrors              : 0
dot3StatsDeferredTransmissions      : 0
dot3StatsLateCollisions             : 0
dot3StatsExcessiveCollisions        : 0
dot3StatsInternalMacTransmitErrors  : 0
dot3StatsCarrierSenseErrors         : 0
dot3StatsFrameTooLongs              : 0
dot3StatsInternalMacReceiveErrors   : 0

linkChange                          : 1


Switch#
```

Display Parameters

rxHCTotalPkts	Receive Packet Counter. Incremented for each packet received (includes bad packets, all Unicast, Broadcast, Multicast Packets, and MAC control packets).
txHCTotalPkts	Transmit Packet Counter. Incremented for each packet transmitted (including bad packets, all Unicast, Broadcast, Multicast packets and MAC control packets).
rxHCUnicastPkts	Receive Unicast Packet Counter. Incremented for each good unicast packet received.
txHCUnicastPkts	Transmit Unicast Packet Counter. Incremented for each good unicast packet transmitted.
rxHCMulticastPkts	Receive Multicast Packet Counter. Incremented for each good Multicast packet received. (Excluding MAC control packets).
txHCMulticastPkts	Transmit Multicast Packet Counter. Incremented for each good Multicast packet transmitted. (Excluding MAC control frames).
rxHCBroadcastPkts	Receive Broadcast Packet Counter. Incremented for each good Broadcast packet received.
txHCBroadcastPkts	Transmit Broadcast Packet Counter. Incremented for each good Broadcast packet transmitted.
rxHCOctets	Receive Byte Counter. Incremented by the byte count of packets received, including bad packets. (Excluding framing bits but including FCS bytes). **Note:** For truncated packet, the counter only counts up to max-rcv-frame-size.
txHCOctets	Transmit Byte Counter. Incremented for the bytes of packets transmitted. (Excluding framing bits but including FCS bytes).
rxHCPkt64Octets	Receive 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes).

rxHCPkt65to127Octets	Receive 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt128to255Octets	Receive 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt256to511Octets	Receive 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len /Type error) frame received which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt512to1023Octets	Receive 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt1024to1518Octets	Receive 1024 to 1518 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 1024 to 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt1519to1522Octets	Receive 1519 to 1522 Byte Good VLAN Frame Counter. Incremented for each good VLAN (excludes FCS, Symbol, Truncated error) frame received which is 1519 to 1522 bytes in length inclusive (excluding framing bits but including FCS bytes). Counts both single and double tag frames.
rxHCPkt1519to2047Octets	Receive 1519 to 2047 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 1519 to 2047 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt2048to4095Octets	Receive 2048 to 4095 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 2048 to 4095 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt4096to9216Octets	Receive 4096 to 9216 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 4096 to 9216 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxHCPkt9217to16383Octets	Receive 9217 to 16383 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame received which is 9217 to 16383 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt64Octets	Transmit 64 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 64 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt65to127Octets	Transmit 65 to 127 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 65 to 127 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt128to255Octets	Transmit 128 to 255 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 128 to 255 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt256to511Octets	Transmit t 256 to 511 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 256 to 511 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt512to1023Octets	Transmit 512 to 1023 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 512 to 1023 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1024to1518Octets	Transmit 1024 to 1518 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 1024 to 1518 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1519to1522Octets	Transmit 1519 to 1522 Byte Good VLAN Frame Counter. Incremented for each good VLAN (excludes FCS and TX errors) frame transmitted which is 1519 to 1522 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt1519to2047Octets	Transmit 1519 to 2047 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 1519 to 2047 bytes in length inclusive (excluding framing bits but including FCS bytes).

txHCPkt2048to4095Octets	Transmit 2048 to 4095 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 2048 to 4095 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt4096to9216Octets	Transmit 4096 to 9216 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 4096 to 9216 bytes in length inclusive (excluding framing bits but including FCS bytes).
txHCPkt9217to16383Octets	Transmit 9217 to 16383 Byte Frame Counter. Incremented for each good or bad (includes FCS, Symbol, Len/Type error) frame transmitted which is 9217 to 16383 bytes in length inclusive (excluding framing bits but including FCS bytes).
rxCRCAlignErrors	Receive Alignment Error Frame Counter. Incremented for each packet received which is 64 to max-rcv-frame-size (or max-rcv-frame-size+4 for tagged frames) octets in length (excluding framing bits, but including FCS octets), but had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxUndersizedPkts	Receive Undersize Frame Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contains a valid FCS).
rxOversizedPkts	Receive Oversized Frame Counter. Incremented for each packet received which is longer than 1518 bytes in length (excluding framing bits, but including FCS octets) and is otherwise well formed (contains a valid FCS). **Note:** Whether oversized frame could be counted is ASIC dependent.
rxFragmentPkts	Receive Fragment Counter. Incremented for each packet received which is less than 64 bytes in length (excluding framing bits but including FCS octets) and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error).
rxJabbers	Receive Jabber Frame Counter. Incremented for each packet received which is longer than 1518 bytes in length (excluding framing bits, but including FCS octets), and had either a bad FCS with an integral number of octets (FCS Error) or a bad FCS with a non-integral number of octets (Alignment Error). **Note:** Whether rxJabbers could be counted is ASIC dependent.
rxSymbolErrors	Receive Code Error Frame Counter. Incremented for the count of times where there was an invalid data symbol when a valid carrier was present.
rxBufferFullDropPkts	Receive Discard Packet Counter. Incremented for each packet discarded for input buffer (GBP) full or back pressure discard.
rxACLDropPkts	Receive ACL Drop Packet Counter. Incremented for each packet dropped by ACL rules.
rxMulticastDropPkts	Receive Multicast Drop Packet Counter. Incremented for each multicast (L2+L3) packets that was dropped.
rxVLANIngressCheckDropPkts	Receive VLAN Drop Packet Counter. Incremented for each packets dropped by VLAN ingress checking.
rxIpv6DropPkts	Receive IPv6 L3 Drop Packet Counter. Incremented for each packet addressed to L3 interface, which are discarded due to the following reasons: RX Buffer hits the Receive Discard Limit or GBP full.
rxSTPDropPkts	Receive STP Drop Packet Counter. Incremented for packets dropped because the Spanning Tree State of the ingress port was not in the forwarding state.
rxStormAndTableDropPkts	Receive Policy Discard Packet Counter. Incremented for packets dropped due to the receive policy: storm control action, FDB action, and so on.
rxMTUDropPkts	Receive MTU Check Error Frame Counter. Incremented for each frame received which exceeds the max-rcv-frame-size in length and contain a valid or invalid FCS. **Note:** Single VLAN tagged, truncation happens at max-rcv-frame-size +4; double VLAN tagged, truncation happens at max-rcv-frame-size +8.
txCollisions	Transmit Total Collision Counter. Incremented by the total number of collisions experienced during the transmission.

ifInErrors	Received Error Packet Counter. Incremented for received packets which contained errors preventing them from being deliverable to a higher-layer protocol. The counter is the sum of dot3StatsAlignmentErrors, dot3StatsFCSErrors, dot3StatsFrameTooLongs, dot3StatsInternalMacReceiveErrors, dot3StatsSymbolErrors, undersize, fragment, oversize, and jabber error.
ifOutErrors	Transmit Error Packet Counter. Incremented for outbound packets which could not be transmitted because of errors. The counter is the sum of dot3StatsSQETestErrors, dot3StatsLateCollisions, dot3StatsExcessiveCollisions, dot3StatsInternalMacTransmitErrors and dot3StatsCarrierSenseErrors.
ifInDiscards	Receive Discards Packet Counter. Incremented for packets received which are dropped due to any condition. Such as MTU drop, Buffer Full Drop, ACL Drop, Multicast Drop, VLAN Ingress Drop, Invalid IPv6, STP Drop, Storm and FDB Discard, and etc.
ifOutDiscards	Transmit Discards Packet Counter. Incremented for packets transmitted which are dropped due to any condition. Such as excessive transit delay discards, HOL drop, STP drop, MTU drop, VLAN drop, and etc.
ifInUnknownProtos	Receive Discards Unknown and Unsupported protocol Counter .Incremented for packets received, which were discarded because of an unknown or unsupported protocol.
txDelayExceededDiscards	Transmit Multiple Deferral Packet Counter. Incremented for packets transmitted which are discarded due to excessive transit delay.
txCRC	Transmit FCS Error Packet Counter. Incremented for each frame transmitted which does not pass the FCS check.
txSTPDropPkts	Transmit STP Drop Packet Counter. Incremented for packets dropped because the Spanning Tree State of the egress port was not in the forwarding state.
txHOLDropPkts	Transmit HOL Drop Packet Counter. Incremented for each packet dropped due to Head Of Line blocking.
dot3StatsAlignmentErrors	Receive Alignment Error Frame Counter. Incremented for each frame received which are not an integral number of octets in length and does not pass the FCS check.
dot3StatsFCSErrors	Receive FCS Error Frame Counter. Incremented for each packet received which is an integral number of octets in length but do not pass the FCS check.
dot3StatsSingleColFrames	Transmit Single Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted which experienced exactly one collision during transmission.
dot3StatsMultiColFrames	Transmit Multiple Collision Frame Counter. 10/100 mode only—incremented for each frame successfully transmitted for which transmission is inhibited by more than one collision.
dot3StatsSQETestErrors	SQET Test Error Counter. Incremented for times that the SQE TEST ERROR message is generated by the PLS sublayer for a particular interface. The SQE TEST ERROR message is defined in section 7.2.2.2.4 of ANSI/IEEE 802.3-1985 and its generation is described in section 7.2.4.6 of the same document. Note: This counter does not increment at speeds greater than 10 Mb/s or in full-duplex mode.
dot3StatsDeferredTransmissions	Transmit Single Deferral Frame Counter. 10/100 mode only—incremented for each frame which was deferred on its first transmission attempt and did not experience any subsequence collisions during transmission.
dot3StatsLateCollisions	Transmit Late Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted which experienced a late collision during a transmission attempt.
dot3StatsExcessiveCollisions	Transmit Excessive Collision Frame Counter. 10/100 mode only—incremented for each frame transmitted for which transmission fails due to excessive collisions.

dot3StatsInternalMacTransmitErrors	Transmit Internal MAC Error Frame counter. Incremented for frames for which transmission fails due to an internal MAC sublayer transmitting error. A frame is only counted if it is not counted by any of the dot3StatsLateCollisions, the dot3StatsExcessiveCollisions, and the dot3StatsCarrierSenseErrors.
dot3StatsCarrierSenseErrors	False Carrier Counter. Incremented for times that the carrier sense condition was lost or never asserted when attempting to transmit a frame.
dot3StatsInternalMacTransmitErrors	Transmit Internal MAC Error Frame counter. Incremented for frames for which transmission fails due to an internal MAC sublayer transmitting error. A frame is only counted if it is not counted by any of the dot3StatsLateCollisions, the dot3StatsExcessiveCollisions, and the dot3StatsCarrierSenseErrors.
dot3StatsFrameTooLongs	Receive Frame Too Long Counter. Incremented for each frame received which exceeds the max-rcv-frame-size.
dot3StatsInternalMacReceiveErrors	Receive Internal MAC Error counter. Incremented for frames for which reception fails due to an internal MAC sublayer receiving error. A frame is only counted if it is not counted by the corresponding instance of any of the dot3StatsFrameTooLongs, the dot3StatsAlignmentErrors, or the dot3StatsFCSErrors.

41-6 show interfaces

This command is used to display the interface information.

show interfaces [*INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 VLAN 1.

```
Switch#show interfaces vlan 1

vlan1 is enabled, Link status is up
  Interface type: VLAN
  Interface description:
  MAC address: 80-26-89-15-28-00



Switch#
```

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

```
Switch#show interfaces loopback 1

loopback1 is enabled, Link status is up
  Interface type: Loopback
  Interface description: Loopback 1 for MIS



Total Entries: 1

Switch#
```

This example shows how to display the NULL interface information for interface null0.

```
Switch#show interfaces null 0

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 port 1.

```
Switch#show interfaces eth1/0/1

eth1/0/1 is enabled link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: 80-26-89-15-28-01
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 100Mb/s
  Maximum transmit unit: 1536 bytes
  RX rate: 0 bytes/sec, TX rate: 0 bytes/sec
  RX bytes: 31953789, TX bytes: 2114661
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 29103, TX packets: 15446
  RX multicast: 1830, RX broadcast: 2981
  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. **(DGS-1520-28 and DGS-1520-52 Only)**

```
Switch#show interfaces mgmt 0

mgmt_ipif 0 is enabled, Link status is up
  Interface type: Management port
  Interface description:

Switch#
```

41-7 show interfaces counters

This command is used to display counters on specified interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] counters [errors]**

show interfaces [*INTERFACE-ID* **[, | -]] counters history {15_minute [slot** *INDEX***] | 1_day [slot** *INDEX***]}**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID to be displayed. If no interface is specified, the counters on all interfaces will be displayed. The interface can only be physical port, port-channel, or L2VLAN interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
errors	(Optional) Specifies to display the error counters. If this parameter is not specified, the general statistics counters will be displayed. Only physical port and port-channel interfaces are allowed.
INTERFACE-ID	(Optional) Specifies the interface ID to be displayed. If no interface is specified, the counters on all interfaces will be displayed. The interface can only be a physical port interface.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
history	Specifies to display the history counters.
15_minute	(Optional) Specifies to display the 15-minute-based historical statistics count.
slot *INDEX*	(Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 5.
1_day	(Optional) Specifies to display the daily-based historical statistics count.
slot *INDEX*	(Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 2.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command allows the user to display general, error or historical statistics counters for the specified or all interfaces.

A particular rate statistics of a port-channel is the sum of all physical member port interface rate for that port-channel. For example, physical ports 1 to 4 belong to the same port-channel, the RX rate (packets per second) of each port is 100, 200, 200,100. As a result, the CRC error packets of the port-channel is 600 packets per second.

There are two kinds of statistics offered for the historical utilization statistics: 15-minute based and 1-day based. For 15-minute based statistics, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago, and so on. For 1-day based statistics, slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

Example

This example shows how to display switch port RX counters on ports 1 to 2.

```
Switch#show interfaces eth1/0/1-2 counters

Port          InOctets /             InMcastPkts /
              InUcastPkts            InBcastPkts
------------- ---------------------- ----------------------
eth1/0/1      12414924               4786
              54604                  12638
eth1/0/2      0                      0
              0                      0

Port          OutOctets /            OutMcastPkts /
              OutUcastPkts           OutBcastPkts
------------- ---------------------- ----------------------
eth1/0/1      14009021               249
              40466                  282
eth1/0/2      0                      0
              0                      0

Total Entries:2


Switch#
```

This example shows how to display switch ports error counters.

```
Switch#show interfaces eth1/0/1,1/0/3 counters errors

Port          Align-Err /            Fcs-Err /
              Rcv-Err /              Undersize /
              Xmit-Err               OutDiscard
------------- ---------------------- ----------------------
eth1/0/1      0                      0
              0                      0
              0                      0
eth1/0/3      0                      0
              0                      0
              0                      0

Port          Single-Col /           Excess-Col /
              Multi-Col /            Carri-Sen /
              Late-Col               Runts
------------- ---------------------- ----------------------
eth1/0/1      0                      0
              0                      0
              0                      0
eth1/0/3      0                      0
              0                      0
              0                      0

Port          Giants /               DeferredTx /
              Symbol-Err /           IntMacTx /
              SQETest-Err            IntMacRx
------------- ---------------------- ----------------------
eth1/0/1      0                      0
              0                      0
              0                      0
eth1/0/3      0                      0
              0                      0
              0                      0

Total Entries:2


Switch#
```

Display Parameters

Align-Err	Refer to the item “dot3StatsAlignmentErrors” in Display Parameters in the **show counters** command.
Fcs-Err	Refer to the item “dot3StatsFCSErrors” in Display Parameters in the **show counters** command.
Rcv-Err	Refer to the item “ifInErrors” in Display Parameters in the **show counters** command.
UnderSize	Refer to the item “rxUndersizedPkts” in Display Parameters in the **show counters** command.
Xmit-Err	Refer to the item “ifOutErrors” in Display Parameters in the **show counters** command.
OutDiscard	Refer to the item “ifOutDiscards” in Display Parameters in the **show counters** command.

Single-Col	Refer to the item “dot3StatsSingleColFrames” in Display Parameters in the **show counters** command.
Multi-Col	Refer to the item “dot3StatsMultiColFrames” in Display Parameters in the **show counters** command.
Late-Col	Refer to the item “dot3StatsLateCollisions” in Display Parameters in the **show counters** command.
Excess-Col	Refer to the item “dot3StatsExcessiveCollisions” in Display Parameters in the **show counters** command.
Carri-Sen	Refer to the item “dot3StatsCarrierSenseErrors” in Display Parameters in the **show counters** command.
Runts	Incremented for each packet whose size is less than 64 bytes in length.
Giants	Incremented for each packet whose size is greater than 1518 bytes in length.
Symbol-Err	Refer to the item “rxSymbolErrors” in Display Parameters in the **show counters** command.
SQETst-Err	Refer to the item “dot3StatsSQETestErrors” in Display Parameters in the **show counters** command.
DeferredTx	Refer to the item “txDelayExceededDiscards” in Display Parameters in the **show counters** command.
IntMacTx	Refer to the item “dot3StatsInternalMacTransmitErrors” in Display Parameters in the **show counters** command.
InMacRx	Refer to the item “dot3StatsInternalMacReceiveErrors” in Display Parameters in the **show counters** command.

This example shows how to display the 15-minute statistics count of port 1.

```
Switch#show interfaces eth1/0/1 counters history 15_minute slot 1

eth1/0/1  15-Minute Slot 1 :
Starttime : 1  Jan 2019  01:44:38
Endtime   : 1  Jan 2019  01:29:38
rxHCTotalPkts                      : 3974
txHCTotalPkts                      : 3317
rxHCUnicastPkts                    : 3292
txHCUnicastPkts                    : 3303
rxHCMulticastPkts                  : 280
txHCMulticastPkts                  : 0
rxHCBroadcastPkts                  : 402
txHCBroadcastPkts                  : 14
rxHCOctets                         : 1617308
txHCOctets                         : 869791
rxHCPkt64Octets                    : 514
rxHCPkt65to127Octets               : 123
rxHCPkt128to255Octets              : 1213
rxHCPkt256to511Octets              : 1069
rxHCPkt512to1023Octets             : 670
rxHCPkt1024to1518Octets            : 385
rxHCPkt1519to1522Octets            : 0
rxHCPkt1519to2047Octets            : 0
rxHCPkt2048to4095Octets            : 0
rxHCPkt4096to9216Octets            : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41-8 show interfaces status

This command is used to display the port connection status of the Switch.

show interfaces [*INTERFACE-ID* **[, | -]] status**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to display the port connection status of the Switch. If no parameter is specified, the connection status of all switch ports will be displayed.

Example

This example shows how to display the Switch's port connection status.

```
Switch#show interfaces status

Port          Status        VLAN         Duplex  Speed          Type
------------- ------------- ------------ ------- -------------- -------------
eth1/0/1      connected     1            a-full  a-100          1000BASE-T
eth1/0/2      not-connected 1            auto    auto           1000BASE-T
eth1/0/3      connected     1            a-full  a-100          1000BASE-T
eth1/0/4      not-connected 1            auto    auto           1000BASE-T
eth1/0/5      not-connected 1            auto    auto           1000BASE-T
eth1/0/6      not-connected 1            auto    auto           1000BASE-T
eth1/0/7      not-connected 1            auto    auto           1000BASE-T
eth1/0/8      not-connected 1            auto    auto           1000BASE-T
eth1/0/9      not-connected 1            auto    auto           1000BASE-T
eth1/0/10     not-connected 1            auto    auto           1000BASE-T
eth1/0/11     not-connected 1            auto    auto           1000BASE-T
eth1/0/12     not-connected 1            auto    auto           1000BASE-T
eth1/0/13     not-connected 1            auto    auto           1000BASE-T
eth1/0/14     not-connected 1            auto    auto           1000BASE-T
eth1/0/15     not-connected 1            auto    auto           1000BASE-T
eth1/0/16     not-connected 1            auto    auto           1000BASE-T
eth1/0/17     not-connected 1            auto    auto           1000BASE-T
eth1/0/18     not-connected 1            auto    auto           1000BASE-T
eth1/0/19     not-connected 1            auto    auto           1000BASE-T
eth1/0/20     not-connected 1            auto    auto           1000BASE-T
eth1/0/21     not-connected 1            auto    auto           2500BASE-T
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41-9 show interfaces utilization

This command is used to display the utilization of the specified port(s) on the Switch.

show interfaces [*INTERFACE-ID* **[, | -]] utilization [history {15_minute [slot** *INDEX***] | 1_day [slot** *INDEX***]}]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID to be displayed. If no interface is specified, the utilization of all physical port interfaces will be displayed. The interface can be physical port or port-channel interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional)Specifies a range of interfaces. No space is allowed before or after the hyphen.
utilization	Specifies to display the utilization information.
history	(Optional) Specifies to display the historical interfaces utilization information. This parameter is only available for the physical port interface.
15_minute	(Optional) Specifies to display the 15-minute-based historical statistics count.
slot *INDEX*	(Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 5.
1_day	(Optional) Specifies to display the daily-based historical statistics count.

slot *INDEX*	(Optional) Specifies the slot number. Slot 1 displays the most recent historical statistics. If the slot number is not specified, all the historical statistics from all the slots will be displayed. The value is from 1 to 2.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

The command allows the user not only to view the utilization for all interfaces or specified interfaces, but also to view the Switch historical CPU and Memory utilization.

A particular rate statistics of a port-channel is the sum of all physical member port interface rate for that port-channel. For example, physical ports 1 to 4 belong to the same port-channel, the RX rate (packets per second) of each port is 100, 200, 200,100. As a result, the CRC error packets of the port-channel is 600 packets per second.

For the historical utilization statistics, there are two kinds of statistics offered, 15-minute based and 1-day based. For statistics based on 15-minute, slot 1 represents the time from 15 minutes ago until now, slot 2 represents the time from 30 minutes ago until 15 minutes ago and so on. For statistics based on 1-day, the slot 1 represents the time from 24 hours ago until now and slot 2 represents the time from 48 hours ago until 24 hours ago.

Example

This example shows how to display the utilization of all the ports on the Switch.

```
Switch#show interfaces utilization

Port           TX packets/sec    RX packets/sec    Utilization
-------------  ----------------- ----------------- -----------
eth1/0/1       0                 0                 0
eth1/0/2       0                 0                 0
eth1/0/3       0                 0                 0
eth1/0/4       0                 0                 0
eth1/0/5       0                 0                 0
eth1/0/6       0                 0                 0
eth1/0/7       0                 0                 0
eth1/0/8       0                 0                 0
eth1/0/9       0                 0                 0
eth1/0/10      0                 0                 0
eth1/0/11      0                 0                 0
eth1/0/12      0                 0                 0
eth1/0/13      0                 0                 0
eth1/0/14      0                 0                 0
eth1/0/15      0                 0                 0
eth1/0/16      0                 0                 0
eth1/0/17      0                 0                 0
eth1/0/18      0                 0                 0
eth1/0/19      0                 0                 0
eth1/0/20      0                 0                 0
eth1/0/21      0                 0                 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the historical utilization on port 1 in 15-minute slots.

```
Switch#show interfaces eth1/0/1 utilization history 15_minute


eth1/0/1  Utilization:
9  Apr 2018  14:56:13 - 9  Apr 2018  14:41:13  : 0   %
9  Apr 2018  14:41:13 - 9  Apr 2018  14:26:13  : 0   %
9  Apr 2018  14:26:13 - 9  Apr 2018  14:11:13  : 0   %
9  Apr 2018  14:11:13 - 9  Apr 2018  13:56:13  : 0   %
9  Apr 2018  13:56:13 - 9  Apr 2018  13:41:13  : 0   %

Switch#
```

41-10 show interfaces gbic

This command is used to display GBIC status information.

show interfaces [*INTERFACE-ID* **[, | -]] gbic**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the GBIC status information on all GBIC interfaces will be displayed.

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays GBIC status information.

Example

This example shows how to display GBIC status information.

```
Switch#show interfaces eth1/0/1 gbic

eth1/0/1
 Interface Type: 1000BASE-T


Switch#
```

41-11 show interfaces auto-negotiation

This command is used to display detailed auto-negotiation information of physical port interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] auto-negotiation**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the auto-negotiation information on all physical port interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
auto-negotiation	Specifies to display detailed auto-negotiation information.

Default

None.

Command Mode

User/Privileged EXEC 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 eth1/0/1 auto-negotiation

eth1/0/1
 Auto Negotiation: Enabled

 Remote Signaling: Detected
 Configure Status: Complete
 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: 10M_Half, 10M_Full, 100M_Half, 100M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


Switch#
```

41-12 show interfaces description

This command is used to display the description and link status of interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] description**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, information related to all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
description	Specifies to display the description and link status of interfaces.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is available for physical port, port-channel, L2VLAN, and VLAN interface configuration.

Use this command to display the description and link status of interfaces.

Example

This example shows how to display the description and link status of interfaces.

```
Switch#show interfaces description

 Interface              Status    Administrative  Description
 ---------------------  --------  --------------  ------------------------------
 eth1/0/1               up        enabled
 eth1/0/2               down      enabled
 eth1/0/3               down      enabled
 eth1/0/4               down      enabled
 eth1/0/5               down      enabled
 eth1/0/6               down      enabled
 eth1/0/7               down      enabled
 eth1/0/8               down      enabled
 eth1/0/9               down      enabled
 eth1/0/10              down      enabled         Physical Port 10
 eth1/0/11              down      enabled
 eth1/0/12              down      enabled
 eth1/0/13              down      enabled
 eth1/0/14              down      enabled
 eth1/0/15              down      enabled
 eth1/0/16              down      enabled
 eth1/0/17              down      enabled
 eth1/0/18              down      enabled
 eth1/0/19              down      enabled
 eth1/0/20              down      enabled
 eth1/0/21              down      enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

41-13 shutdown

This command is used to disable an interface. Use the **no** form of this command to enable an interface.

shutdown

no shutdown

Parameters

None.

Default

By default, this option is **no shutdown**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is available for physical port, loopback, VLAN, and MGMT interface configuration. This command is also available for port channel member ports.

The command will cause the port to enter the disabled state. Under the disabled state, the port will not be able to receive or transmit any packets. Using the **no shutdown** command will put the port back into the enabled state. When a port is shut down, the link status will also be turned off.

Example

This example shows how to disable the port state on port 1.

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

41-14 max-rcv-frame-size

This command is used to configure the maximum Ethernet frame size allowed. Use the **no** form of this command to revert to the default setting.

max-rcv-frame-size *BYTES*

no max-rcv-frame-size

Parameters

BYTES	Specifies the maximum Ethernet frame size allowed. The range is from 64 to 12288 bytes.

Default

By default, this value is 1536 bytes.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port and port-channel interface configuration. Oversize frames will be dropped and checks are carried out on ingress ports. Use this command to transfer large frames or jumbo frames through the Switch to optimize server-to-server performance.

Example

This example shows how to configure the maximum received Ethernet frame size to be 6000 bytes on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#max-rcv-frame-size 6000
Switch(config-if)#
```

42. Internet Group Management Protocol (IGMP) Commands

42-1 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#
```

42-2 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 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)#
```

42-3 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 revert 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)#
```

42-4 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 enable IGMP and 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)#
```

42-5 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 this 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)#
```

42-6 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 this 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

Use this command to configure 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)#
```

42-7 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 setting.

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)#
```

42-8 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 this 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

Use this command 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)#
```

42-9 ip igmp version

This command is used to change the IGMP version on the specified interface. Use the **no** form of this command to revert to the default setting.

ip igmp version *NUMBER*

no ip igmp version

Parameters

NUMBER	Specifies the IGMP version. **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, the setting configured by the **ip igmp query-max-response-time** command will not be effective.

Example

This example shows how to enable IGMP and 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)#
```

42-10 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/Privileged EXEC 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, 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.

42-11 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 an interface. 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/Privileged EXEC 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 VLAN1.

```
Switch#show ip igmp interface vlan1

VLAN 1
  Version                      : 3
  IP Address/Netmask           : 172.18.67.139/21
  IGMP State                   : Enabled
  Querier                      : 172.18.67.139
  Query Interval               : 125 seconds
  Query Maximum Response Time  : 10 seconds
  Robustness Variable          : 2
  Last Member Query Interval   : 1 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. **Enabled** indicates not to ignore the source IP check. **Disabled** indicates to ignore the source IP check.

43. Internet Group Management Protocol (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 this option.

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/Privileged EXEC 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/Privileged EXEC 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/Privileged EXEC 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. Internet Group Management Protocol (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 VLANs.

The IGMP snooping global state is disabled.

Command Mode

VLAN Configuration Mode.

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This function must be enabled in both Global Configuration Mode and VLAN Configuration Mode for a VLAN to operate with MLD snooping. IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

Example

This example shows how to enable the IGMP snooping operation on all VLANs.

```
Switch#configure terminal
Switch(config)#ip igmp snooping
Switch(config)#
```

This example shows how to disable IGMP snooping on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#no ip igmp snooping
Switch(config-vlan)#
```

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. Use the **no** form of this command to disable this function.

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 *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 this command on the Switch 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.

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

Example

This example shows how to restrict the serviced IGMP snooping group to 226.1.1.1 on port 1. In the following example, first, create an IP access list named “igmp_filter” which only permits the packets destined for the group address 226.1.1.1. Then, associate this access group with port 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#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping access-group igmp_filter
Switch(config-if)#
```

44-4 ip igmp snooping accounting

This command is used to enable accounting when a listener joining an IGMP group. Use the **no** form to disable the function.

ip igmp snooping accounting

no ip igmp snooping accounting

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 physical port and port-channel interface configuration. Use this command to enable or disable accounting when a listener joining an IGMP group. When enabled and the client joins a group, the accounting message will be sent to RADIUS.

Example

This example shows how to enable IGMP accounting on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping accounting
Switch(config-if)#
```

44-5 ip igmp snooping authentication

This command is used to enable authentication function for IGMP join messages. Use the **no** form to disable the function.

ip igmp snooping authentication

no ip igmp snooping authentication

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 physical port and port-channel interface configuration. Use this command to enable or disable authentication function for IGMP join messages. When enabled and the client wants to join a group, the system will perform authentication first.

Example

This example shows how to enable authentication function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping authentication
Switch(config-if)#
```

44-6 ip igmp snooping fast-leave

This command is used to configure IGMP snooping fast-leave on the interface. Use the **no** form of this command 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

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to allow 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. When enabled, the Switch will not generate specific queries. When disabled, the Switch will generated specific queries.

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)#
```

44-7 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** form of this 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

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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)#
```

44-8 ip igmp snooping last-member-query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP group-specific or group-source-specific (channel) query messages. Use the **no** form of this command to revert to the default setting.

ip igmp snooping last-member-query-interval *SECONDS*

no ip igmp snooping last-member-query-interval

Parameters

SECONDS	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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)#
```

44-9 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 512.
exceed-action	(Optional) Specifies the action for handling newly learned groups when the limitation is exceeded.
drop	(Optional) Specifies that the new group will be dropped.
replace	(Optional) Specifies that the new group will replace the oldest group.
except *ACCESS-LIST-NAME*	(Optional) 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), specifies S in the source address field and G in the destination address field of the access list entry. To permit a group (*,G), specifies “any” in the source address field and G in the destination address field of the access list entry.
vlan *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN 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.

Example

This example shows how to set the limit number of IGMP snooping groups with a configuration limit from an ACL that port 4 with the VLAN ID of 1000 can join to.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#ip igmp snooping limit 80 except igmp_filter 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 with the VLAN ID of 1000 can join to.

```
Switch#configure terminal
Switch(config)#interface port-channel 4
Switch(config-if)#no ip igmp snooping limit vlan 1000
Switch(config-if)#
```

44-10 ip igmp snooping mrouter

This command is used to configure the specified interface(s) as the multicast router ports or as forbidden to be multicast router ports on the Switch. Use the **no** form of this command to remove the interface(s) from router ports or forbidden multicast router ports.

ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

no ip igmp snooping mrouter {interface *INTERFACE-ID* **[, | -] | forbidden interface** *INTERFACE-ID* **[, | -]}**

Parameters

interface	Specifies a static multicast router port.
forbidden interface	Specifies a port that cannot be multicast router port.
INTERFACE-ID	Specifies an interface or an interface list. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No IGMP snooping multicast router port is configured.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be member port of the configured VLAN. A multicast router port can be either dynamic learned or statically configured. With the dynamic learning, the IGMP snooping entity will learn IGMP, PIM, or DVMRP packet to identify a multicast router port.

Example

This example shows how to 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 eth1/0/4
Switch(config-vlan)#
```

44-11 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

source *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

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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, 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-vlan)#ip igmp snooping proxy-reporting source 1.2.2.2
Switch(config-vlan)#
```

44-12 ip igmp snooping querier

This command is used to enable the capability of the entity as an IGMP querier. Use the **no** form of this command to disable the querier function.

ip igmp snooping querier

no ip igmp snooping querier

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the system can play the querier role, the entity will listen for IGMP query packets sent by other devices. If IGMP query message is received, the device with lower value of IP address becomes the querier. 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)#
```

44-13 ip igmp snooping query-interval

This command is used to configure the interval at which the IGMP snooping querier sends IGMP general query messages periodically. Use the **no** form of this command to revert to the default setting.

ip igmp snooping query-interval *SECONDS*

no ip igmp snooping query-interval

Parameters

SECONDS	Specifies to configure the interval at which the designated router sends IGMP general-query messages. The range is 1 to 31744.

Default

By default, this value is 125 seconds

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The query interval is the interval between General Queries sent by the Querier. By varying the query interval, an administrator may tune the number of IGMP messages on the network; larger values cause IGMP Queries to be sent less often.

Example

This example shows how to configure the IGMP snooping query interval to 300 seconds on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping query-interval 300
Switch(config-vlan)#
```

44-14 ip igmp snooping query-max-response-time

This command is used to configure the maximum response time advertised in IGMP snooping queries. Use the **no** form of this command to revert to the default setting.

ip igmp snooping query-max-response-time *SECONDS*

no ip igmp snooping query-max-response-time

Parameters

SECONDS	Specifies to set the maximum response time, in seconds, advertised in IGMP snooping queries. The range is 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the period of which the group member can respond to an IGMP query message before the IGMP Snooping deletes the membership.

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)#
```

44-15 ip igmp snooping query-version

This command is used to configure the general query packet version sent by the IGMP snooping querier. Use the **no** form of this command to revert to the default setting.

ip igmp snooping query-version *NUMBER*

no ip igmp snooping query-version

Parameters

NUMBER	Specifies the version of the IGMP general query sent by the IGMP snooping querier. The value is from 1 to 3.

Default

By default, this value is 3.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The query version number setting will affect the querier electing. When configured to version 1, IGMP snooping will always act as the querier, and will not initiate new querier electing no matter what IGMP query packet is received. When configured to version 2 or version 3, IGMP snooping will initiate a new querier electing if any IGMPv2 or IGMPv3 query packet is received. When receiving an IGMPv1 query packet, IGMP snooping 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)#
```

44-16 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. The value is from 1 to 1000.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In the Interface Configuration Mode, this command is only available for physical port and port-channel interface configuration. Use this command to configure 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip igmp snooping rate-limit 30
Switch(config-if)#
```

This example shows how to limit 30 packets per second on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping rate-limit 30
Switch(config-vlan)#
```

44-17 ip igmp snooping report-suppression

This command is used to enable the report suppression. Use the **no** form of this command to disable the report suppression.

ip igmp snooping report-suppression

no ip igmp snooping report-suppression

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The report suppression function only works for IGMPv1 and IGMPv2 traffic. When report suppression is enabled, the Switch suppresses the duplicate reports sent by hosts. The suppression for the same group report or leave will continue until the suppression time expired. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.

Example

This example shows how to enable report suppression on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip igmp snooping report-suppression
Switch(config-vlan)#
```

44-18 ip igmp snooping robustness-variable

This command is used to set the robustness variable used in IGMP snooping. Use the **no** form of this command to revert to the default setting.

ip igmp snooping robustness-variable *VALUE*

no ip igmp snooping robustness-variable

Parameters

VALUE	Specifies the robustness variable. The value is from 1 to 7.

Default

By default, this value is 2.

Command Mode

VLAN 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.

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)#
```

44-19 ip igmp snooping static-group

This command is used to configure an IGMP snooping static group. Use the **no** form of this command is used to delete a static group.

ip igmp snooping static-group *GROUP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ip igmp snooping static-group *GROUP-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

GROUP-ADDRESS	Specifies an IP multicast group address.
interface *INTERFACE-ID*	Specifies the interfaces to be displayed. Only physical port and port-channel interfaces are allowed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

By default, no static-group is configured.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create an IGMP snooping static group in case that the attached host does not support the IGMP protocol.

Example

This example shows how to statically add a group 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 eth1/0/5
Switch(config-vlan)#
```

44-20 ip igmp snooping suppression-time

This command is used to configure the time for suppressing duplicate IGMP reports or leaves. Use the **no** form of this command to revert to the default setting.

ip igmp snooping suppression-time *SECONDS*

no ip igmp snooping suppression-time

Parameters

SECONDS	Specifies to configure the time for suppressing duplicates IGMP reports. The range is from 1 to 300.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The report suppression function will suppress the duplicate IGMP report or leave packets received in the suppression time. A small suppression time will cause the duplicate IGMP packets be sent more frequently.

Example

This example shows how to configure the suppression time to be 125 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ip igmp snooping suppression-time 125
Switch(config-vlan)#
```

44-21 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 *NUMBER*

no ip igmp snooping minimum-version

Parameters

NUMBER	**2:** Specifies to filter out IGMPv1 messages. **3:** Specifies to filter out IGMPv1 and IGMPv2 messages.

Default

By default, there is no limit on the minimum version.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This setting only applies to the filtering of IGMP membership reports.

Example

This example shows how to restrict all IGMPv1 hosts to join.

```
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)#
```

44-22 show ip igmp snooping

This command is used to display IGMP snooping information on the Switch.

show ip igmp snooping [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

User/Privileged EXEC 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

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                  : Disabled (Source 0.0.0.0)
    Rate limit                       : 0
    Ignore topology change           : Disabled

Total Entries: 1

Switch#
```

44-23 show ip igmp snooping aaa

This command is used to display IGMP snooping authentication and accounting configuration information.

show ip igmp snooping aaa [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display IGMP snooping authentication and accounting configuration information. If no optional parameter is specified, information for all interfaces will be displayed.

Example

This example shows how to display IGMP snooping authentication and accounting configuration information.

```
Switch#show ip igmp snooping aaa

Authentication enabled interface:
1/0/1-1/0/5

Accounting enabled interface:
1/0/1-1/0/5

Switch#
```

44-24 show ip igmp snooping groups

This command is used to display IGMP snooping dynamic group information learned on the Switch.

show ip igmp snooping groups [vlan *VLAN-ID* **[, | -] | [***IP-ADDRESS***] [detail]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN interface to be displayed. If no VLAN is specified, IGMP snooping group information of all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
IP-ADDRESS	(Optional) Specifies the group IP address to be displayed. If no IP address is specified, all IGMP group information will be displayed.
detail	(Optional) Specifies to display the IGMP group detail information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display IGMP snooping dynamic group information.

Example

This example shows how to display IGMP snooping dynamic group information.

```
Switch#show ip igmp snooping groups

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5

Switch#
```

This example shows how to display IGMP snooping group detail information.

```
Switch#show ip igmp snooping groups detail

Total Group Entries : 1
Total Source Entries: 2

vlan1, 230.1.1.1
Learned on port: 1/0/3,1/0/5
  1/0/3
    version: v2, filter mode: Exclude, uptime: 0DT00H00M05S, expires: 0DT00H04M16S
  1/0/5
    version: v3, filter mode: Include, uptime: 0DT00H00M07S, expires: 0DT00H00M00S
      source 192.168.1.1, uptime: 0DT00H00M07S, expires: 0DT00H04M13S

Switch#
```

44-25 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 *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.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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


eth1/0/1
    Rate limit: Not Configured
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: AccessList, exceed-action: drop)

eth1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

This example shows how to display filter information of port 2.

```
Switch#show ip igmp snooping filter interface eth1/0/2


eth1/0/2
    Rate limit: 10pps
    Access group: Not Configured
    Groups/Channel Limit: Not Configured
    vlan1:
      Access group: Not Configured
      Groups/Channel Limit: 100 (Exception List: ExtendACL, exceed-action: drop)

Switch#
```

44-26 show ip igmp snooping mrouter

This command is used to display IGMP snooping multicast router information that has been automatically learned and manually 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.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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       1/0/1-1/0/4 (static)

Total Entries: 1

Switch#
```

44-27 show ip igmp snooping statistics

This command is used to display IGMP snooping statistics information on the Switch.

show ip igmp snooping statistics {interface [*INTERFACE-ID* **[, | -]] | vlan [***VLAN-ID* **[, | -]]}**

Parameters

interface	Specifies to display statistics counters by interface.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan	Specifies to display statistics counters by VLAN.
VLAN-ID	(Optional) Specifies the VLAN ID to be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 0, Query 0
  IGMPv2 Rx: Report 0, Query 0, Leave 0
  IGMPv3 Rx: Report 3, Query 0
  IGMPv1 Tx: Report 0, Query 0
  IGMPv2 Tx: Report 0, Query 0, Leave 0
  IGMPv3 Tx: Report 1, Query 2

Total Entries: 1

Switch#
```

44-28 show ip igmp snooping static-group

This command is used to display statically configured IGMP snooping groups on the Switch.

show ip igmp snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IP address to be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display statically configured IGMP snooping groups on the Switch. If no optional parameter is specified, all information will be displayed.

Example

This example shows how to display statically configured IGMP snooping groups.

```
Switch#show ip igmp snooping static-group

VLAN ID  Group address    Interface
-------  ---------------  ------------------------
1        230.1.1.1        1/0/1-1/0/2

Total Entries: 1

Switch#
```

45. IP Multicast (IPMC) Commands

45-1 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#
```

45-2 ip multicast table-lookup-mode

This command is used to configure the IP multicasting forwarding lookup mode. Use the **no** form of this command to revert to the default setting.

ip multicast table-lookup-mode {ip | mac}

no ip multicast table-lookup-mode

Parameters

ip	Specifies that multicasting forwarding look up is based on IP address.
mac	Specifies that multicasting forwarding look up is based on MAC address.

Default

By default, this function is based on IP address.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the IP multicasting forwarding lookup mode.

Example

This example shows how to configure the IP multicasting forwarding lookup mode to mac.

```
Switch#configure terminal
Switch(config)#ip multicast table-lookup-mode mac
Switch(config)#
```

45-3 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)#
```

45-4 ip multicast boundary

This command is used to avoid leaking the limited scoped multicast traffic in private domain across the domain boundary interfaces. Use the **no** form of this command to delete the boundary.

ip multicast boundary *ACCESS-LIST* **[in | out]**

no ip multicast boundary *ACCESS-LIST* **[in | out]**

Parameters

ACCESS-LIST	Specifies a standard IP access list which includes a list of permitted (*,G) or (S,G) entries, or denied (*,G) or (S,G) entries.
in	(Optional) Specifies to filter the multicast user traffic that arrives at the interface based on the specified access list. This filters the multicast traffic for the specific group traffic, or the specific groups from the specific source.
out	(Optional) Specifies to filter the PIM join message or IGMP join message that arrives at the interface. This filtering prevents the interface from becoming an outgoing interface for the denied (*,G) or (S,G) entries.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command only takes effect when PIM is enabled, and only one access list can be specified for each direction. If no optional parameter is specified, the access list filtering will apply to both in and out directions.

Example

This example shows how to configure VLAN1 as a boundary interface to filter the traffic based on the access list, StandIPACL.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip multicast boundary StandIPACL
Switch(config-if)#
```

45-5 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, 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)#
```

45-6 cpu-filter l3-control-pkt

This command is used to discard the layer 3 control packets sent to CPU form the specific ports. Use the **no** form of this command to stop discarding the layer 3 control packets sent to CPU.

cpu-filter l3-control-pkt type [*PACKET-TYPE***]**

no cpu-filter l3-control-pkt type [*PACKET-TYPE***]**

Parameters

PACKET-TYPE	(Optional) Specifies layer 3 control packet to be configured. The supported layer 3 control packet types are: • **dvmrp:** Distance Vector Multicast Routing Protocol. • **igmp-query:** Internet Group Management Protocol Query. • **ospf:** Open Shortest Path First Protocol. • **pim:** Protocol Independent Multicast. • **rip:** Routing Information Protocol • **vrrp:** Virtual Router Redundancy Protocol.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to discard the layer 3 control packets sent to CPU form the specific ports.

Example

This example shows how to discard DVMRP packets sent to CPU.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#cpu-filter l3-control-pkt type dvmrp
Switch(config-if)#
```

45-7 show cpu-filter l3-control-pkt

This command is used to display the layer 3 control packet CPU filtering status.

show cpu-filter l3-control-pkt [interface *INTERFACE-ID***]**

Parameters

INTERFACE-ID	(Optional) Specifies an interface. The interface can be a physical interface or a port-channel. If not specified, IGMP snooping filter information on all interfaces will be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the layer 3 control packet CPU filtering status.

Example

This example shows how to display the layer 3 control packet CPU filtering status.

```
Switch#show cpu-filter l3-control-pkt


eth1/0/2
    Filter packet: DVMRP

Switch#
```

45-8 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/Privileged EXEC 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 and the IP multicasting forwarding lookup mode.

```
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

vlan2
  Internet address is 192.168.2.109/24
  Multicast routing: enabled, PIM Sparse mode
  Multicast boundary: not set

vlan3
  Internet address is 192.168.3.109/24
  Multicast routing: enabled, PIM Sparse mode
  Multicast boundary: not set

vlan4
  Internet address is 192.168.4.109/24
  Multicast routing: enabled, PIM Sparse mode
  Multicast boundary: not set


Total Entries: 3

Switch#
```

45-9 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 a 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/Privileged EXEC 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: 192.168.8.0/24, RPF neighbor: NULL

 Total Entries   : 2

Switch#
```

45-10 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/Privileged EXEC 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, port-channel2

(*,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#
```

45-11 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/Privileged EXEC 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.

45-12 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/Privileged EXEC 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#
```

46. IP Multicast Version 6 (IPMCv6) Commands

46-1 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)#
```

46-2 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 **interface** parameter is not specified, the state of IPv6 multicast routing will be displayed.

Default

None.

Command Mode

User/Privileged EXEC 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, the information for all IPv6 interfaces will be displayed.

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. **PIM-DM:** PIM Dense Mode is enabled on this interface.

46-3 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***] | dense | sparse | summary]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IPv6 address.
SOURCE-ADDRESS	(Optional) Specifies the multicast source IPv6 address.
dense	(Optional) Specifies to display only the PIM-DM routes.
sparse	(Optional) Specifies to display only the PIM-SM routes.
summary	(Optional) Specifies to display a one-line, abbreviated summary of each entry in the IPv6 multicast routing table.

Default

None.

Command Mode

User/Privileged EXEC 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. 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 parameter 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: 3 entries
Flags: S - Sparse, D - Dense, s - SSM Group
Timers: Uptime/Expires

(2000::1010:134, FF07::1), vlan1, 0DT00H01M32S/0DT00H03M20S, Flags: S
(2000::2001:101, FF06::100), vlan10, 0DT00H05M10S/0DT00H03M11S, Flags: S
(2000::5001:101, FF1E::100), vlan100, 0DT00H04M10S/0DT00H04M11S, Flags: D

Switch#
```

This example shows how to display multicast route entries.

```
Switch#show ipv6 mroute

IPv6 Multicast Routing Table - 3 entries
Flags: S - Sparse, D - Dense, s - SSM Group
Timers: Uptime/Expires

(2000::1010:134, FF07::1), 0DT05H29M15S/0DT00H02M59S, Flags: S
    Incoming interface: vlan1
    RPF nbr: 2000::103:405
    Outgoing interface list:
      vlan2
      vlan3

(2000::2001:101, FF06::20), 0DT05H29M15S/0DT00H02M59S  Flags: S
    Incoming interface: vlan10
    RPF nbr: 2000::1003:405
    Outgoing interface list:
      vlan20

(2000::5001:101, FF1E::100), 0DT00H04M10S/0DT00H04M11S, Flags: D
    Incoming interface: vlan100
    RPF nbr: -
    Outgoing interface list:
      vlan200

Switch#
```

Display Parameters

Flags	Provides information about the entry. S - Sparse. Entry is operating in sparse mode. D – Dense. Entry is operating in dense mode. s - SSM Group. The Entry is SSM group.
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.

46-4 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/Privileged EXEC 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, port-channel2

(2000:60:1:1::10, FF0E::1:1:2) VLAN0060
  Outgoing interface list: 1/0/1, 2/0/2

Total entries: 2

Switch#
```

46-5 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/Privileged EXEC 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#
```

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.
Metric	Indicates the unicast routing metric. This field is optional if the metric does not exist.

47. IP Source Guard Commands

47-1 ip verify source vlan dhcp-snooping

This command is used to enable IP source guard for a port. Use the **no** form of this command to disable IP source guard.

ip verify source vlan dhcp-snooping [ip-mac]

no ip verify source vlan dhcp-snooping [ip-mac]

Parameters

ip-mac	(Optional) Specifies to check both IP address and MAC address of the received IP packets.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to enable the IP source guard on the configured port.

When a port is enabled for IP source guard, the IP packet that arrives at the port will be validated via the port ACL. Port ACL is a hardware mechanism and its entry can come from either a manual configured entry or the DHCP snooping binding database. The packet that fails to pass the validation will be dropped.

When a VLAN is enabled for IP source guard, the IP packet that arrives at a member port will be validated. It will allow hosts that belong to the IP inspection group to roam in the specified VLAN domain between member ports.

There are two types of validations.

- If **ip-mac** is not specified, the validation is based on the source IP address and VLAN check only.
- If **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 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip verify source vlan dhcp-snooping
Switch(config-if)#
```

47-2 ip source binding

This command is used to create a static entry used for IP source guard. Use the **no** form of this command to delete a static binding entry.

ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ip source binding *MAC-ADDRESS* **vlan** *VLAN-ID IP-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

Parameters

MAC-ADDRESS	Specifies the MAC address of the IP-to-MAC address binding entry.
vlan *VLAN-ID*	Specifies the VLAN that the valid host belongs to.
IP-ADDRESS	Specifies the IP address of the IP-to-MAC address binding entry.
interface *INTERFACE-ID*	Specifies the port that the valid host is connected.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

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 port 10.

```
Switch#configure terminal
Switch(config)#ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

This example shows how to delete an IP Source Guard entry with the IP address 10.1.1.1 and MAC address 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch#configure terminal
Switch(config)#no ip source binding 00-01-02-03-04-05 vlan 2 10.1.1.1 interface eth1/0/10
Switch(config)#
```

47-3 show ip source binding

This command is used to display an IP-source guard binding entry.

show ip source binding [*IP-ADDRESS***] [***MAC-ADDRESS***] [dhcp-snooping | static] [vlan** *VLAN-ID***] [interface** *INTERFACE-ID* **[, | -]]**

Parameters

IP-ADDRESS	(Optional) Specifies to display the IP-source guard binding entry based on IP address.
MAC-ADDRESS	(Optional) Specifies to display the IP-source guard binding entry based on MAC address.
dhcp-snooping	(Optional) Specifies to display the IP-source guard binding entry learned by DHCP binding snooping.
static	(Optional) Specifies to display the IP-source guard binding entry that is manually configured.
vlan *VLAN-ID*	(Optional) Specifies to display the IP-source guard binding entry based on VLAN.
interface *INTERFACE-ID*	(Optional) Specifies to display the IP-source guard binding entry based on ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 all IP Source Guard binding entries.

```
Switch#show ip source binding

MAC Address       IP Address      Lease(sec)  Type         VLAN Interface
----------------- --------------- ---------- ------------- ---- ---------
00-01-01-01-01-01 10.1.1.10        infinite  static        100  eth1/0/3
00-01-01-01-01-10 10.1.1.11          3120    dhcp-snooping 100  eth1/0/3

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    eth1/0/3

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 port 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
eth1/0/3

MAC Address       IP Address      Lease(sec)  Type         VLAN   Interface
----------------- --------------- ---------- ------------- ----- -----------
00-01-01-01-01-10 10.1.1.11          3564    dhcp-snooping 100    eth1/0/3

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.

47-4 show ip verify source

This command is used to display the hardware port ACL entry on a particular interface.

show ip verify source [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip          active      10.1.1.1        -                 100
eth1/0/3        ip          active      deny-all        -                 101-120

Total Entries: 2

Switch#
```

This example shows how to display when the interface has an IP source filter mode that is configured as IP MAC and an existing IP MAC that binds IP address 10.1.1.10 to MAC address 00-01-01-01-01-01 on VLAN 100 and IP address 10.1.1.11 to MAC address 00-01-01-01-01-10 on VLAN 101.

```
Switch#show ip verify source interface eth1/0/3

Interface       Filter-type Filter-mode IP address      MAC address       VLAN
---------       ----------- ----------- --------------- ----------------- ----
eth1/0/3        ip-mac      active      10.1.1.10       00-01-01-01-01-01 100
eth1/0/3        ip-mac      active      10.1.1.11       00-01-01-01-01-10 101
eth1/0/3        ip-mac      active      deny-all               -          102-120

Total Entries: 3

Switch#
```

Display Parameters

Interface	The interface that has IP inspection enabled.
Filter-type	The type of IP Source Guard in operation. **ip:** Only 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.

48. IP Utility Commands

48-1 ping

This command is used to diagnose basic network connectivity.

ping {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [count** *TIMES***] [timeout** *SECONDS***] [source {***IP-ADDRESS* **|** *IPV6-ADDRESS***}]**

Parameters

ip	(Optional) Specifies to use the IPv4 address.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
ipv6	(Optional) Specifies to use the IPv6 address.
IPV6-ADDRESS	Specifies the IPv6 address of the system to discover. If the IPv6 address is a link-local address or a multicast address, the IP interface name needs to be specified in the following format: *IPV6-ADDRESS***%***INTERFACE-ID*.
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***}**	(Optional) Specifies the source IP address used for the ping packet. The specified IP address must one of the IP address configured for the Switch. The destination address and the source IP must be the same type of address, both are IPv4 or IPv6.

Default

The **count** value is disabled. The ping will continue until the user terminates the process.

The **timeout** value is 1 second.

Command Mode

User/Privileged 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. To terminate the ping before it has finished, press CTRL+C. Up to five active ping sessions are supported.

Example

This example shows how to ping the host with IP address 172.50.71.123.

```
Switch#ping 172.50.71.123 count 5

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 =5, Received =5, 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 count 3

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 =3, Received =3, Lost =0

Switch#
```

48-2 ping access-class

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

ping access-class *IP-ACL*

no ping access-class *IP-ACL*

Parameters

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

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 10.1.1.1 is allowed to ping the Switch.

```
Switch#configure terminal
Switch(config)#ip access-list ping-filter
Switch(config-ip-acl)#permit 10.1.1.1 0.0.0.0
Switch(config-ip-acl)#exit
Switch(config)#ping access-class ping-filter
Switch(config)#
```

48-3 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 {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS* **|** *HOST-NAME***} [probe** *NUMBER***] [timeout** *SECONDS***] [max-ttl** *TTL***] [port** *DEST-PORT***]**

Parameters

ip	(Optional) Specifies to use the IPv4 address.
IP-ADDRESS	Specifies the IPv4 address of the destination host.
ipv6	(Optional) Specifies to use the IPv6 address.
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 1000.
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 255.
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 1 to 65535. Use this option in the unlikely event that the destination host is listening to a port in the default trace-route port range.

Default

The **probe** value (query number for each TTL) is 1.

The timeout period is 5 seconds.

The maximum TTL value is 30.

The destination base UDP port number is 33434.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

To terminate the traceroute before it has finished, press CTRL+C. Up to three active traceroute sessions are supported.

This command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. A **traceroute** 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 **traceroute** 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, **traceroute** 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, **traceroute** 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 **traceroute** facility that it has reached the destination.

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 max-ttl 2

  *      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

Trace complete.


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#
```

48-4 ip helper-address

This command is used to add a target address for the forwarding of UDP broadcast packets. Use the **no** form of this 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

None.

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)#
```

48-5 ip forward-protocol

This command is used to enable the forwarding of a specific UDP service type of packets. Use the **no** form of this 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, 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
Switch(config)#
```

48-6 show ip helper-address

This command is used to display UDP helper address table.

show ip helper-address [*INTERFACE-ID***]**

Parameters

INTERFACE-ID	(Optional) Specifies the VLAN's interface ID that will be used for the display. If no interface ID is specified, all related interfaces' information will be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display UDP helper address table.

Example

This example shows how to display UDP helper address table.

```
Switch#show ip helper-address

Interface   Helper-address
----------  ---------------
vlan100     172.50.71.123

Switch#
```

48-7 show ip forward-protocol udp

This command is used to display all specified UDP ports' information.

show ip forward-protocol udp

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all specified UDP ports' information.

Example

This example shows how to display all specified UDP ports' information.

```
Switch#show ip forward-protocol udp

Application                  UDP Port
-------------------          ---------------
Time Service                 37
IEN-116 Name Service         42
TACACS                       49
TFTP                         69
NetBIOS-NS                   137
NetBIOS-DS                   138

Switch#
```

49. IP-MAC-Port Binding (IMPB) Commands

49-1 clear ip ip-mac-port-binding violation

This command is used to clear IMPB blocked entries.

clear ip ip-mac-port-binding violation {all | interface *INTERFACE-ID* **|** *MAC-ADDRESS***}**

Parameters

all	Specifies to clear all of the violation entries.
interface *INTERFACE-ID*	Specifies to clear the violation entries created by the specified interface.
MAC-ADDRESS	Specifies to clear the violation entries of the specified MAC address.

Default

None.

Command Mode

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 port 4.

```
Switch#clear ip ip-mac-port-binding violation interface eth1/0/4
Switch#
```

49-2 ip ip-mac-port-binding

This command is used to enable the IMPB access control for port interfaces. Use the **no** form of this command to disable the IMPB access control function.

ip ip-mac-port-binding [*MODE***]**

no ip ip-mac-port-binding

Parameters

MODE	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 port 10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/10
Switch(config-if)#ip ip-mac-port-binding strict
Switch(config-if)#
```

49-3 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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
violation	(Optional) Specifies to display the blocked entry.

Default

None.

Command Mode

User/Privileged EXEC 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
------- --------- ------------------
eth1/0/3      1       01-00-0c-cc-cc-cc
eth1/0/3      1       01-80-c2-00-00-00
eth1/0/4      1       01-00-0c-cc-cc-cd
eth1/0/4      1       01-80-c2-00-00-01

Total Entries: 4

Switch#
```

This example shows how to display the IMPB configuration for all ports.

```
Switch#show ip ip-mac-port-binding

Port           Mode
---------- ------------
eth1/0/1       Strict
eth1/0/2       Strict
eth1/0/3       Loose
eth1/0/4       Loose

Total Entries: 4

Switch#
```

49-4 snmp-server enable traps ip-mac-port-binding

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

snmp-server enable traps ip-mac-port-binding

no snmp-server enable traps ip-mac-port-binding

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When IMPB notifies that state is enabled, the Switch will send violation traps if any violation packet is received. Use this command to enable or disable the sending of SNMP notifications for such events.

Example

This example shows how to enable the sending of traps for IMPB.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps ip-mac-port-binding
Switch(config)#
```

50. IPv6 Snooping Commands

50-1 ipv6 snooping policy

This command is used to create or modify an IPv6 snooping policy. This command will enter the IPv6 snooping configuration mode. Use the **no** form of this command to delete an IPv6 snooping policy.

ipv6 snooping policy *POLICY-NAME*

no ipv6 snooping policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the name of the snooping policy.

Default

No IPv6 snooping policy is created.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an IPv6 snooping policy and enter the IPv6 snooping configuration mode. 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)#
```

50-2 protocol

This command is used to specify the protocol that IPv6 snooping should be enabled for. Use the **no** form of this command to disable snooping for the specific protocol.

protocol {dhcp | ndp | dhcp-pd | dhcp-pd-ext}

no protocol {dhcp | ndp | dhcp-pd | dhcp-pd-ext}

Parameters

dhcp	Specifies that addresses should be snooped in DHCPv6 packets.
ndp	Specifies that addresses should be snooped in NDP packets.
dhcp-pd	Specified that IPv6 prefix should be snooped in DHCPv6 PD packets.

dhcp-pd-ext	Specified that IPv6 prefix should be snooped in DHCPv6 PD packets. PD snooping runs in the extension mode.

Default

By default, all protocols are disabled.

Command Mode

IPv6 Snooping Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Neighbor Discovery (ND) snooping is designed for IPv6 stateless address auto-configuration and manually configured IPv6 addresses. Before assigning an IPv6 address, the host must perform Duplicate Address Detection (DAD) first. ND snooping detects DAD messages, which include DAD Neighbor Solicitation (NS) and DAD Neighbor Advertisement (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 assignment procedure. When a DHCPv6 client successfully gets a valid IPv6 address, DHCPv6 snooping creates its binding database.

DHCP-PD snooping sniffs DHCPv6 Prefix Delegation (PD) packets between the Delegating Router (assigned IPv6 prefix) and corresponding Requesting Router to set up prefix bindings.

The following modes are supported in PD Snooping:

- **Standard Mode:** The DHCPv6 Request/Confirm (with Reply) packet triggers PD Snooping to set up a new binding entry. The DHCPv6 Renew (with Reply) packet triggers PD Snooping to specify a new lease time for the existing binding entry.
- **Extension Mode:** The DHCPv6 Request/Confirm Renew/Rebind (with Reply) packet triggers PD Snooping to set up a new binding entry. The DHCPv6 Renew (with Reply) packet triggers PD Snooping to specify a new lease time for the existing binding entry.

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)#
```

50-3 data-glean

This command is used to enable the data gleaning function. Use the **no** form of this command to revert to the default setting.

data-glean

no data-glean

Parameters

None.

Default

By default, this option is disabled.

Command Mode

IPv6 Snooping Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Switches sometimes encounter the valid address lost in binding table for some devices and the traffic of those devices is denied by IPv6 source guard. The data gleaning function provides a method for the Switch to recover those lost IPv6 addresses via IPv6 Duplicate Address Detection (DAD).

Example

This example shows how to enable the data gleaning function.

```
Switch#configure terminal
Switch(config)#ipv6 snooping policy policy1
Switch(config-ipv6-snooping)#data-glean
Switch(config-ipv6-snooping)#
```

50-4 limit address-count

This command is used to limit the maximum number of IPv6 snooping binding entries. Use the **no** form of this command to revert to the default setting.

limit address-count *MAXIMUM*

no limit address-count

Parameters

MAXIMUM	Specifies the maximum number of IPv6 snooping binding entries. The range is from 0 to 511.

Default

By default, there is no limit configured.

Command Mode

IPv6 Snooping Configuration Mode.

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)#
```

50-5 ipv6 snooping attach-policy

This command is used to apply an IPv6 snooping policy to a specified VLAN. Use the **no** form of this command to remove the binding.

ipv6 snooping policy attach-policy *POLICY-NAME*

no ipv6 snooping policy attach-policy

Parameters

POLICY-NAME	Specifies the name of the snooping policy.

Default

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)#vlan 200
Switch(config-vlan)#ipv6 snooping attach-policy policy1
Switch(config-vlan)#
```

50-6 ipv6 snooping station-move deny

This command is used to deny the station move function for IPv6 snooping entries. Use the **no** form of this command to revert to the default setting.

ipv6 snooping station-move deny

no ipv6 snooping station-move deny

Parameters

None.

Default

By default, the station move function is permitted.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When station move is permitted, the dynamic snooping binding entry with the same VLAN ID and MAC address on the specific port can move to another port if the following conditions are detected:

- 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)#
```

50-7 ipv6 neighbor binding max-entries

This command is used to configure the maximum number of IPv6 snooping entries. Use the **no** form of this command to revert to the default setting.

ipv6 neighbor binding max-entries {dhcp | ndp | dhcp-pd} *NUMBER*

no ipv6 neighbor binding max-entries {dhcp | ndp | dhcp-pd}

Parameters

dhcp	Specifies the maximum number of entries for DHCPv6 snooping.
ndp	Specifies the maximum number of entries for ND snooping.
dhcp-pd	Specifies the maximum number of entries for DHCPv6 PD snooping.
NUMBER	Specifies the maximum number of entries. The value is between 0 and 511. Specifies 0 to disable learning on the specified port.

Default

The default value is 511.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to configure the maximum number of IPv6 snooping entries. Each snooping protocol has its own setting.

Example

This example shows how to configure the maximum number of DHCPv6 snooping entries to 10 on port 1.

```
Switch#configure terminal
Switch(config)#interface ethernet 1/0/1
Switch(config-if)#ipv6 neighbor binding max-entries dhcp 10
Switch(config-if)#
```

50-8 clear ipv6 snooping entries

This command is used to clear IPv6 snooping entries on the specified interface.

clear ipv6 snooping entries {dhcp | ndp | dhcp-pd} interface *INTERFACE-ID* **[, | -]**

Parameters

dhcp	Specifies to clear DHCPv6 snooping entries.
ndp	Specifies to clear ND snooping entries.
dhcp-pd	Specifies to clear DHCPv6 PD snooping entries.
interface *INTERFACE-ID*	Specifies the interface ID.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear IPv6 snooping entries on the specified interface.

Example

This example shows how to clear IPv6 snooping entries on port 1.

```
Switch#clear ipv6 snooping entries ndp interface eth1/0/1
Switch#
```

50-9 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 to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display DHCPv6 guard information. If no parameter is specified, information is displayed for all policies.

Example

This example shows how to display DHCPv6 guard information.

```
Switch#show ipv6 snooping policy

Snooping policy: policy1
    Protocol: DHCP
    Data Glean: Enabled
    Limit Address Count: 25
    Target VLAN: 200

Switch#
```

Display Parameters

Protocol	The protocol used for snooping.
Data Glean	The status of the data gleaning function.
Limit Address Count	The maximum allowed number of entries in this IPv6 Snooping policy.
Target VLAN	The name of the target. The target is a VLAN list.

51. IPv6 Source Guard Commands

51-1 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. When configuring this command, the specified VLAN does not need to be an existing VLAN. If the specified interface is removed later, the configuration of this command will be removed accordingly.

Example

This example shows how to configure an IPv6 Source Guard entry with the IPv6 address of 2000::1 and MAC address of 00-01-02-03-04-05 at VLAN 2 on port 10.

```
Switch#configure terminal
Switch(config)#ipv6 source binding 00-01-02-03-04-05 vlan 2 2000::1 interface eth1/0/1
Switch(config)#
```

51-2 ipv6 source-guard policy

This command is used to create an IPv6 source guard policy and enter into the Source-guard Policy Configuration Mode. Use the **no** form of this command to remove an IPv6 source guard policy.

ipv6 source-guard policy *POLICY-NAME*

no ipv6 source-guard policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the name of the source guard policy.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create or remove a source guard policy name. This command will enter into the Source-guard Policy Configuration Mode.

Example

This example shows how to create an IPv6 source guard policy.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#
```

51-3 deny global-autoconfig

This command is used to deny auto-configured traffic. Use the **no** form of this command to disable this function.

deny global-autoconfig

no deny global-autoconfig

Parameters

None.

Default

By default, this option is permitted.

Command Mode

Source-guard Policy Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to deny data traffic from auto-configured global addresses. It is useful when all global addresses on a link are assigned by DHCP and the administrator 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)#
```

51-4 permit link-local

This command is used to allow hardware permitted data traffic to be sent 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 or disable hardware to permit data traffic sent by the link-local address.

Example

This example shows how to allow all data traffic that is sent 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)#
```

51-5 validate address

This command is used to enable the IPv6 source guard function to perform the validate address feature. Use the **no** form of this command to disable the validate address feature.

validate address

no validate address

Parameters

None.

Default

By default, this feature is enabled.

Command Mode

Source-guard Policy Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable the IPv6 source guard function to perform the validate address feature.

Example

This example shows how to disable the validate address feature.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#no validate address
Switch(config-source-guard)#
```

51-6 validate prefix

This command is used to enable the IPv6 source guard function to perform the IPv6 prefix-guard operation. Use the **no** form of this command to disable this feature.

validate prefix

no validate prefix

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Source-guard Policy Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to enable the IPv6 source guard function to perform the IPv6 prefix-guard operation.

Example

This example shows how to enable the IPv6 source guard function to perform the IPv6 prefix guard operation.

```
Switch#configure terminal
Switch(config)#ipv6 source-guard policy policy1
Switch(config-source-guard)#validate prefix
Switch(config-source-guard)#
```

51-7 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 the source guard from the interface.

ipv6 source-guard attach-policy [*POLICY-NAME***]**

no ipv6 source-guard attach-policy

Parameters

POLICY-NAME	(Optional) Specifies the name of the source guard policy.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

When the command is applied to a port, the received IPv6 packet except ND, RA, RS and DHCP messages will perform the address binding check. The packet is allowed when it matches any entry in the address binding table. The binding table includes the dynamic table (created by IPv6 snooping commands) and the static table (created by the **ipv6 source binding vlan** command).

When the command is applied to a VLAN, it allows hosts that belong to the IP inspection group to roam in the specified VLAN domain between member ports.

If the policy name is not specified, the default source guard policy will permit packets sent by the auto-configured address and deny packets sent by the link-local address.

Example

This example shows how to apply the IPv6 source guard policy “pol1” to port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 source-guard attach-policy pol1
Switch(config-if)#
```

51-8 show ipv6 source-guard policy

This command is used to display the IPv6 source guard policy configuration.

show ipv6 source-guard policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the source guard policy.

Default

None.

Command Mode

User/Privileged EXEC 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 displayed.

Example

This example shows how to display the IPv6 source guard policy configuration.

```
Switch#show ipv6 source-guard policy

Policy policy1 configuration:
    Target: eth1/0/3

Switch#
```

51-9 show ipv6 neighbor binding

This command is used to display the IPv6 binding table.

show ipv6 neighbor binding [vlan *VLAN-ID***] [interface** *INTERFACE-ID***] [ipv6** *IPV6-ADDRESS***] [mac** *MAC-ADDRESS***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies to display the binding entries that match the specified VLAN.
interface *INTERFACE-ID*	(Optional) Specifies to display the binding entries that match the specified interface number.
ipv6 *IPV6-ADDRESS*	(Optional) Specifies to display the binding entries that match the specified IPv6 address.
mac *MAC-ADDRESS*	(Optional) Specifies to display the binding entries that match the specified MAC address.

Default

None.

Command Mode

User/Privileged EXEC 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, P - DHCP-PD Snooping
  IPv6 address                  MAC address    Interface       VLAN Time left
S 1000::1                       000D.8811.8B6A eth1/0/2        1    N/A
N FE80::A8BB:CCFF:FE01:F500     AABB.CC01.F500 eth1/0/3        100  8850
S FE80::21D:71FF:FE99:4900      001D.7199.4900 eth1/0/4        100  N/A
N 2001:600::1                   AABB.CC01.F500 eth1/0/5        100  3181
D 2001:100::2                   AABB.CC01.F600 eth1/0/6        200  9196
D 2001:400::1                   001D.7199.4900 eth1/0/7        100  1568
S 2001:500::1                   000A.000B.000C eth1/0/8        300  N/A
P 400::/64                                     eth1/0/9        300  1440

Total Entries: 8

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.

52. Layer 2 Protocol Tunnel (L2PT) Commands

52-1 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#
```

52-2 l2protocol-tunnel

This command is used to enable the protocol tunneling for the specified protocols. Use the **no** form of this command to disable the protocol tunneling.

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 Address (DA).
01-00-0c-cc-cc-cd	(Optional) Specifies to tunnel the protocol packets with this 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 Layer 2 protocol packets. 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 tunneling.

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, 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 tunneling.

If the port that is enabled for the Layer 2 protocol tunnel receives an encapsulated packet, 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 eth1/0/1
Switch(config-if)#l2protocol-tunnel stp

 WARNING: STP doesn't run when l2 protocol tunnel is enabled for the port.
Switch(config-if)#
```

52-3 l2protocol-tunnel cos

This command is used to specify the CoS value for tunneling of the protocol packets. Use the **no** form of this command to revert 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 encapsulates 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)#
```

52-4 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 this command to revert 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 DA.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this DA.
PPS	Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets per second.

Default

By default, no threshold is configured.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The tunneling of 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. When the threshold is exceeded, the excessive incoming packets are dropped.

If the 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)#interface eth1/0/1
Switch(config-if)#l2protocol-tunnel drop-threshold stp 2000
Switch(config-if)#
```

52-5 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 this command to revert 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, no threshold is configured.

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)#
```

52-6 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 this command to revert to the default setting.

l2protocol-tunnel shutdown-threshold [gvrp | stp | protocol-mac {01-00-0c-cc-cc-cc | 01-00-0c-cc-cc-cd}] *PPS*

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 DA.
01-00-0c-cc-cc-cd	(Optional) Specifies the protocol packets with this DA.
PPS	Specifies the threshold in number of packets per second This value must be between 1 and 4096 packets.

Default

By default, no threshold is configured.

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 eth1/0/1
Switch(config-if)#l2protocol-tunnel shutdown-threshold stp 200
Switch(config-if)#
```

52-7 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/Privileged EXEC 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            :7
Drop Threshold for Encapsulated Packets :5000

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
---------- ------------ --------- --------- ---------- ---------- ----------
eth1/0/1   stp          3200      2000      0          0          0

Switch#
```

This example shows how to display the protocols that are tunneled on port 1.

```
Switch#show l2protocol-tunnel interface eth1/0/1

Port       Protocol     Shutdown  Drop      Encap      Decap      Drop
                        Threshold Threshold Counter    Counter    Counter
---------- ------------ --------- --------- ---------- ---------- ----------
eth1/0/1   stp          3200      2000      0          0          0

Switch#
```

Display Parameters

CoS for Encapsulated Packets	Indicates the Class of Service (CoS) value for tunneled L2 protocol packets.
Drop Threshold for Encapsulated Packets	Indicates the rate limiting on L2PT.
Protocol	Indicates the type of L2 protocol to be tunneled.
Drop Counter	Indicates the number of specified L2 protocol packets which are dropped.
Port	Indicates the port(s) with L2PT enabled.
Shutdown Threshold	Indicates the shutdown threshold for specified L2 protocol packet.
Drop Threshold	Indicates the drop threshold for the specified L2 protocol packet.
Encap Counter	Indicates the number of L2 protocol packets received and encapsulated by the L2PT-enabled port.
Decap Counter	Indicates the number of L2 protocol packets decapsulated and transmitted to the L2PT-enabled port.

53. Link Aggregation Control Protocol (LACP) Commands

53-1 channel-group

This command is used to assign an interface to a channel group. Use the **no** form of this command to remove an interface from a channel-group.

channel-group *CHANNEL-NO* **mode {on | active | passive}**

no channel-group

Parameters

CHANNEL-NO	Specifies the channel group ID. The valid range is 1 to 32.
on	Specifies that the interface is a static member of the channel-group.
active	Specifies the interface to operate in LACP active mode.
passive	Specifies the interface to operate in LACP passive mode.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.

If the **on** parameter is specified, the channel group type is static. If the **active** or **passive** parameter is specified, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

If the security function is enabled on a port, this port cannot be specified as a channel group member.

Example

This example shows how to assign ports 4 and 5 to a new LACP channel-group, with an ID of 3, and sets the LACP mode to active.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if)#channel-group 3 mode active
Switch(config-if)#
```

53-2 lacp port-priority

This command is used to configure the port priority. Use the **no** form of this command to revert to the default setting.

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 ports 4 and 5.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-5
Switch(config-if)#lacp port-priority 20000
Switch(config-if)#
```

53-3 lacp timeout

This command is used to configure the LACP long or short timer. Use the **no** form of this command to revert to the default setting.

lacp timeout {short | long}

no lacp timeout

Parameters

short	Specifies that there will be 3 seconds before invalidating received LACPDU information and there will be 1 second between LACP PDU periodic transmissions when the link partner uses 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 the link partner uses 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lacp timeout long
Switch(config-if)#
```

53-4 lacp system-priority

This command is used to configure the system priority. Use the **no** form of this command to revert to the default setting.

lacp system-priority *PRIORITY*

no lacp system-priority

Parameters

PRIORITY	Specifies the system priority. The range is 1 to 65535.

Default

The default LACP system-priority is 32768.

Command Mode

Global Configuration Mode.

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. 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)#
```

53-5 port-channel load-balance

This command is used to configure the load-balancing algorithm that the Switch uses to distribute packets across ports in the same channel. Use the **no** form of this command to revert to the default setting.

port-channel load-balance {dst-ip | dst-mac | src-dst-ip | src-dst-mac | src-ip | src-mac | 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 IP destination address and Layer 4 destination TCP/UDP port.
src-dst-l4-port	Specifies that the Switch should examine the IP source address, IP destination address, Layer 4 source TCP/UDP port, and Layer 4 destination port
src-l4-port	Specifies that the Switch should examine the IP source address and Layer 4 source TCP/UDP port.

Default

The default load-balancing 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.

When configuring the load-balance hash key to use IP address (**src-ip**, **dst-ip**, and **src-dst-ip**) or MAC address (**src-mac**, **dst-mac**, and **src-dst-mac**) for load balancing on Link Aggregation Group (LAG) link, the load-balancing calculation will be performed as below according to various packet types.

Example

This example shows how to configure the load-balancing algorithm as **src-ip**.

```
Switch#configure terminal
Switch(config)#port-channel load-balance src-ip
Switch(config)#
```

53-6 show channel-group

This command is used to display the channel group information.

show channel-group [channel [*CHANNEL-NO*] {detail | neighbor} | load-balance | sys-id]

Parameters

channel	(Optional) Specifies to display information for the specified port-channels.
CHANNEL-NO	(Optional) Specifies the channel group ID.
detail	(Optional) Specifies to display detailed channel group information.
neighbor	(Optional) Specifies to display neighbor information.
load-balance	(Optional) Specifies to display the load balance information.
sys-id	(Optional) Specifies to display the system identifier that is being used by LACP.

Default

None.

Command Mode

User/Privileged EXEC 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 3
  Member Ports: 2, Maxports = 12, Protocol: LACP
  Description:
                       LACP         Port       Port
  Port          Flags  State        Priority   Number
  ------------------------------------------------
  eth1/0/4      FA     down         20000      0
  eth1/0/5      FA     down         20000      0

Switch#
```

This example shows how to display the neighbor information for port-channel 3.

```
Switch#show channel-group channel 3 neighbor

Flag:
  S - Port is requesting Slow LACPDUs   F - Port is requesting fast LACPDU
  A - Port is in active mode            P - Port is in passive mode

Channel Group 3
               Partner                  Partner   Partner   Partner
  Port         System ID                PortNo    Flags     Port_Pri
  ------------------------------------------------------------------
  eth1/0/21    32768,F0-7D-68-36-3C-00   21        FA        32768
  eth1/0/22    32768,F0-7D-68-36-3C-00   22        FA        32768
  eth1/0/23        0,00-00-00-00-00-00   0         SP        0
  eth1/0/24        0,00-00-00-00-00-00   0         SP        0

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: 32768,F0-7D-68-34-00-10

Switch#
```

This example shows how to display the summary information for all port-channels.

```
Switch#show channel-group

load-balance algorithm: src-dst-mac enhanced MPLS label
System-ID: 32768,F0-7D-68-30-36-00

Group           Protocol
-----------------------
3               LACP

Switch#
```

54. Link Layer Discovery Protocol (LLDP) Commands

54-1 clear lldp counters

This command is used to delete LLDP statistics.

clear lldp counters [all | interface *INTERFACE-ID* **[, | -]]**

Parameters

all	(Optional) Specifies to clear LLDP counter information for all interfaces and global LLDP statistics.
interface *INTERFACE-ID*	(Optional) Specifies the interface to clear LLDP counter information. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command with the **interface** parameter to reset LLDP statistics of the specified interface(s). Use this command with the **all** parameter to clear global LLDP statistics and the LLDP statistics on all interfaces. If no parameter is specified, only the LLDP global counters will be cleared.

Example

This example shows how to clear all LLDP statistics.

```
Switch#clear lldp counters all
Switch#
```

54-2 clear lldp table

This command is used to delete LLDP information learned from neighboring devices.

clear lldp table {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

all	Specifies to clear LLDP neighboring information for all interfaces.
INTERFACE-ID	Specifies the interface ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command with the **interface** parameter to clear information learned from neighboring devices on the specified interface(s). Use this command with the **all** parameter to clear all information learned from neighboring devices.

Example

This example shows how to clear all neighboring information on all interfaces.

```
Switch#clear lldp table all
Switch#
```

54-3 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 LLDPDUs, and sent to neighbor devices. Use the **no** form of this command to disable the transmission of TLVs.

lldp dot1-tlv-select {port-vlan | 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 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. If no VLAN ID is specified, all configured PPVID VLANs will be cleared and no PPVID TLV will be sent.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
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. If no VLAN ID is specified, all configured VLANs for the VLAN name TLV will be cleared and no VLAN name TLV will be sent.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
protocol-identity	Specifies the Protocol Identity TLV to send. The Protocol Identity TLV is an optional TLV that allows an IEEE 802 LAN station to advertise particular protocols that are accessible through the port.
PROTOCOL-NAME	(Optional) Specifies the protocol name here. The valid strings for *PROTOCOL-NAME* are: **eapol** - Extensible Authentication Protocol (EAP) over LAN **lacp** - Link Aggregation Control Protocol **gvrp** - GARP VLAN Registration Protocol **stp** - Spanning Tree Protocol

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 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, 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 eth1/0/1
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 eth1/0/1
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 eth1/0/1
Switch(config-if)#lldp dot1-tlv-select vlan-name 1-3
Switch(config-if)#
```

This example shows how to enable the LACP Protocol Identity TLV advertisement.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot1-tlv-select protocol-identify lacp
Switch(config-if)#
```

54-4 lldp dot3-tlv-select

This command is used to specify which optional TLVs in the IEEE 802.3 organizationally specific TLV set will be encapsulated in LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]

no lldp dot3-tlv-select [mac-phy-cfg | link-aggregation | power | max-frame-size]

Parameters

mac-phy-cfg	(Optional) Specifies the MAC/PHY configuration/status TLV to send. The MAC/PHY configuration/status TLV is an optional TLV that identifies (1) the duplex and bit-rate capability of the sending IEEE 802.3 LAN node, and (2) the current duplex and bit-rate settings of the sending IEEE 802.3 LAN node.
link-aggregation	(Optional) Specifies the link aggregation TLV to send. The link aggregation TLV 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, the ID is 0.
power	(Optional) Specifies the power via MDI TLV to send. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station.

max-frame-size	(Optional) Specifies the maximum frame size TLV to send. The maximum frame size TLV indicates the maximum frame size capability of the implemented MAC and PHY.

Default

No IEEE 802.3 organizationally specific TLV is selected.

Command Mode

Interface Configuration Mode.

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.

When no optional parameter is specified, all supported IEEE 802.3 organizationally specific TLVs are selected or de-selected in this command.

Example

This example shows how to enable the advertising MAC/PHY Configuration/Status TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp dot3-tlv-select mac-phy-cfg
Switch(config-if)#
```

54-5 lldp fast-count

This command is used to configure the LLDP-MED fast start repeat count option on the Switch. Use the **no** form of this command to revert to the default setting.

lldp fast-count *VALUE*

no lldp fast-count

Parameters

VALUE	Specifies the LLDP-MED fast start repeat count value. This value must be between 1 and 10.

Default

By default, this value is 4.

Command Mode

Global Configuration Mode.

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)#
```

54-6 lldp hold-multiplier

This command is used to configure the hold multiplier for LLDP updates on the Switch. Use the **no** form of this command to revert to the default setting.

lldp hold-multiplier *VALUE*

no hold-multiplier

Parameters

VALUE	Specifies the multiplier on the LLDPDU 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 LLDPDU 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)#
```

54-7 lldp management-address

This command is used to configure the management address that will be advertised on the physical interface. Use the **no** form of this command to remove the settings.

lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

no lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Parameters

IP-ADDRESS	(Optional) Specifies the IPv4 address that is carried in the management address TLV.
IPV6-ADDRESS	(Optional) Specifies the IPv6 address that is carried in the management address TLV.

Default

No LLDP management address is configured (no Management Address TLV is sent).

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration. This command specifies the IPv4/IPv6 address that is carried in the management address TLV on the specified port. If an IP address is specified, but the address is not one of the addresses of the system interfaces, the address will not be sent.

If no parameter is specified, the Switch will find least one IPv4 and IPv6 address of the VLAN with the smallest VLAN ID. If no applicable IPv4/IPv6 address exists, no management address TLV will be advertised. Once the administrator configures an address, both of the default IPv4 and IPv6 management address will become inactive and won't be sent. The default IPv4 or IPv6 address will be active again when all the configured addresses are removed. Multiple IPv4/IPv6 management addresses can be configured by using this command multiple times.

Use the **no lldp management-address** command without a management address to disable the management address adverted in LLDPDUs. If there is no effective management address in the list, no Management Address TLV will be sent.

Example

This example shows how to configure the management IPv4 address on ports 1 to 3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#lldp management-address 10.1.1.1
Switch(config-if-range)#
```

This example shows how to configure the management IPv6 address on ports 4 to 6.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-6
Switch(config-if-range)#lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

This example shows how to remove the management IPv4 address from ports 1 to 3.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-3
Switch(config-if-range)#no lldp management-address 10.1.1.1
Switch(config-if-range)#
```

This example shows how to remove the management IPv6 address from ports 4 to 6.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/4-6
Switch(config-if-range)#no lldp management-address FE80::250:A2FF:FEBF:A056
Switch(config-if-range)#
```

This example shows how to remove all management IPv4/IPv6 addresses from port 5. No management address TLV will be sent from port 5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#no lldp management-address
Switch(config-if)#
```

54-8 lldp med-tlv-select

This command is used to specify which optional LLDP-MED TLV will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to disable the transmission of the TLVs.

lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

no lldp med-tlv-select [capabilities | inventory-management | network-policy | power-management]

Parameters

capabilities	(Optional) Specifies to transmit the LLDP-MED capabilities TLV.
inventory-management	(Optional) Specifies to transmit the LLDP-MED inventory management TLV.
network-policy	(Optional) Specifies to transmit the LLDP-MED network policy TLV.
power-management	(Optional) Specifies to transmit the LLDP-MED extended power via MDI TLV, if the local device is PSE device or PD device.

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. Use this command to enable or disable transmitting LLDP-MED TLVs. If no parameter is specified, all optional LLDP-MED TLVs will be configured.

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.

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 receives LLDP packets only.

Example

This example shows how to enable transmitting LLDP-MED TLVs and LLDP-MED Capabilities TLVs.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp med-tlv-select capabilities
Switch(config-if)#
```

54-9 lldp receive

This command is used to enable a physical interface to receive LLDP messages. Use the **no** form of this command to disable receiving LLDP messages.

lldp receive

no lldp receive

Parameters

None.

Default

LLDP is enabled on all supported interfaces.

Command Mode

Interface Configuration Mode.

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 does not receive LLDP messages.

Example

This example shows how to enable a physical interface to receive LLDP messages.

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

54-10 lldp reinit

This command is used to configure the minimum re-initialization the delay on the Switch. Use the **no** form of this command to revert to the default setting.

lldp reinit *SECONDS*

no lldp reinit

Parameters

SECONDS	Specifies the delay value for LLDP initialization on an interface. This value must be between 1 and 10 seconds.

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

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)#
```

54-11 lldp run

This command is used to enable LLDP globally. Use the **no** form of this command to revert to the default setting.

lldp run

no lldp run

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to globally enable LLDP so that the Switch can start to transmit LLDP packets and receive and process the LLDP packets. 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. 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)#
```

54-12 lldp forward

This command is used to enable the LLDP forwarding state. Use the **no** form of this command to revert to the default setting.

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)#
```

54-13 lldp tlv-select

This command is used to select the TLVs in the 802.1AB basic management set and will be transmitted and encapsulated in the LLDPDUs and sent to neighbor devices. Use the **no** form of this command to revert to the default setting.

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 for the IEEE 802 LAN station's port description to be advertised.
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 eth1/0/1
Switch(config-if)#lldp tlv-select
Switch(config-if)#
```

This example shows how to enable advertising the system name TLV.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp tlv-select system-name
Switch(config-if)#
```

54-14 lldp transmit

This command is used to enable the LLDP advertise (transmit) capability. Use the **no** form of this command to disable LLDP transmission.

lldp transmit

no lldp transmit

Parameters

None.

Default

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 does not transmit LLDP messages.

Example

This example shows how to enable LLDP transmission.

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

54-15 lldp tx-delay

This command is used to configure the transmission delay timer. This delay timer defines the minimum interval between the sending of LLDP messages due to constantly changing MIB content. Use the **no** form of this command to revert to the default setting.

lldp tx-delay *SECONDS*

no lldp tx-delay

Parameters

SECONDS	Specifies the delay value for sending successive LLDPDUs on an interface. The valid values are from 1 to 8192 seconds and should not be greater than one-fourth of the transmission interval timer.

Default

By default, this value is 2 seconds.

Command Mode

Global Configuration Mode.

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)#
```

54-16 lldp tx-interval

This command is used to configure the LLDPDUs transmission interval on the Switch. Use the **no** form of this command to revert to the default setting.

lldp tx-interval *SECONDS*

no lldp tx-interval

Parameters

SECONDS	Specifies the interval between consecutive transmissions of LLDP advertisements on each physical interface. The range is from 5 to 32768 seconds.

Default

By default, this value is 30 seconds.

Command Mode

Global Configuration Mode.

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 LLDP updates to be sent every 50 seconds.

```
Switch#configure terminal
Switch(config)#lldp tx-interval 50
Switch(config)#
```

54-17 snmp-server enable traps lldp

This command is used to enable the sending of LLDP and LLDP-MED notifications. Use the **no** form of this command disable this feature.

snmp-server enable traps lldp [med]

no snmp-server enable traps lldp [med]

Parameters

med	(Optional) Specifies to enable the LLDP-MED trap state.

Default

The LLDP and LLDP-MED trap states are disabled.

Command Mode

Global Configuration Mode.

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)#
```

54-18 lldp notification enable

This command is used to enable the sending of LLDP and LLDP-MED notifications from an interface. Use the **no** form of this command disable this feature.

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 from port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#lldp med notification enable
Switch(config-if)#
```

54-19 lldp subtype

This command is used to configure the subtype of LLDP TLV(s).

lldp subtype port-id {mac-address | local}

Parameters

port-id	Specifies the subtype of the port ID TLV.
mac-address	Specifies the subtype of the port ID TLV as “MAC Address (3)” and the field of “port ID” to be encoded with the MAC address.
local	Specifies the subtype of the port ID TLV as “Locally assigned (7)” and the field of “port ID” to 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 eth1/0/1
Switch(config-if)#lldp subtype port-id mac-address
Switch(config-if)#
```

54-20 show lldp

This command is used to display the general LLDP configuration of the Switch.

show lldp

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the LLDP global configuration of the Switch.

Example

This example shows how to display the LLDP global configuration of the Switch.

```
Switch#show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 80-26-89-15-28-00
    System Name               : Switch
    System Description        : Gigabit Ethernet Smart Managed Switch
    System Capabilities Supported: Repeater, Bridge
    System Capabilities Enabled  : Repeater, Bridge

LLDP-MED System Information:
    Device Class              : Network Connectivity Device
    Hardware Revision         : A1
    Firmware Revision         : 1.00.011
    Software Revision         : 1.01.004
    Serial Number             : DGS1520-28MPA
    Manufacturer Name         : D-Link Corporation
    Model Name                : DGS-1520-28MP
    Asset ID                  :
    PoE Device Type           : PSE Device
    PoE PSE Power Source      : Primary

LLDP Configurations
    LLDP State                : Disabled
    LLDP Forward State        : Disabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

54-21 show lldp interface

This command is used to display the LLDP configuration on the physical interface.

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 the LLDP configuration on port 1.

```
Switch#show lldp interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID                                                 :eth1/0/1
Admin Status                                            :TX and RX
Notification                                            :Disabled
Basic Management TLVs:
    Port Description                                    :Disabled
    System Name                                         :Disabled
    System Description                                  :Disabled
    System Capabilities                                 :Disabled
    Enabled Management Address:
        (None)
IEEE 802.1 Organizationally Specific TLVs:

    Port VLAN ID                                        :Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
IEEE 802.3 Organizationally Specific TLVs:

    MAC/PHY Configuration/Status                        :Disabled
    Power Via MDI                                       :Disabled
    Link Aggregation                                    :Disabled
    Maximum Frame Size                                  :Disabled

LLDP-MED Organizationally Specific TLVs:

    LLDP-MED Capabilities TLV                           :Disabled
    LLDP-MED Network Policy TLV                         :Disabled
    LLDP-MED Extended Power Via MDI PSE TLV             :Disabled
    LLDP-MED Inventory TLV                              :Disabled



Switch#
```

Display Parameters

Enabled Management Address	Displays the enabled IPv4/IPv6 addresses. '(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	Displays enabled port and protocol VLANs. The VLAN list is the configured and enabled VLANs. If there is no configured PPVID VLAN, '(None)' is displayed.
Enabled VLAN Name	Displayed enabled VLANs for sending VLAN Name TLVs. The VLAN list includes the configured and enabled VLANs. If there is no configured VLAN for the VLAN Name TLV, '(None)' is displayed.
Enabled Protocol Identity	Displays the enabled protocol string for protocol identity TLVs. If there is no enabled protocol for the protocol identity TLV, '(None)' is displayed.

54-22 show lldp local interface

This command is used to display physical interface information that will be carried in the LLDP TLVs and sent to neighbor devices.

show lldp local interface *INTERFACE-ID* **[, | -] [brief | detail]**

Parameters

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

```
SSwitch#show lldp local interface eth1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1520-28MP HW
                                           A1 firmware 1.01.004 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                              : 1.3.6.1.4.1.171.10.171.2.1

    Address 2 :
        Subtype                          : IPv4
        Address                          : 10.90.90.90
        IF Type                          : IfIndex
        OID                              : 1.3.6.1.4.1.171.10.171.2.1

PPVID Entries Count                      : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the local information of port 1 in normal mode.

```
Switch#show lldp local interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1520-28MP HW
                                           A1 firmware 1.01.004 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)
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)


Switch#
```

This example shows how to display local information of port 1 in brief mode.

```
Switch#show lldp local interface eth1/0/1 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : eth1/0/1
Port Description                         : D-Link Corporation DGS-1520-28MP HW
                                           A1 firmware 1.01.004 Port 1 on
                                           Unit 1


Switch#
```

54-23 show lldp management-address

This command is used to display the management address information.

show lldp management-address [*IP-ADDRESS* **|** *IPV6-ADDRESS***]**

Parameters

IP-ADDRESS	(Optional) Specifies to display the LLDP management information for a specific IPv4 address.
IPV6-ADDRESS	(Optional) Specifies to display the LLDP management information for a specific IPv6 address.

Default

None.

Command Mode

User/Privileged EXEC 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                              : 1.3.6.1.4.1.171.10.171.2.1
    Advertising Ports                : -

Address 2 :
-----------------------------------------------
    Subtype                          : IPv4
    Address                          : 10.90.90.90
    IF Type                          : IfIndex
    OID                              : 1.3.6.1.4.1.171.10.171.2.1
    Advertising Ports                : -

Total Entries : 2


Switch#
```

54-24 show lldp neighbors interface

This command is used to display the information currently learned from the neighbor on the specific physical interface.

show lldp neighbors interface *INTERFACE-ID* **[, | -] [brief | detail]**

Parameters

INTERFACE-ID	Specifies the interface ID. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
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/Privileged EXEC 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 detailed LLDP information about neighboring devices connected to port 1.

```
Switch#show lldp neighbors interface eth1/0/1 detail

Port ID: eth1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                          : MAC Address
    Chassis ID                                  : 80-26-89-15-28-A0
    Port ID Subtype                             : Local
    Port ID                                     : eth1/0/1
    Port Description                            :
    System Name                                 :
    System Description                          :
    System Capabilities                         :
    Management Address Count                    : 0
        (None)

    Port PVID                                   : 0
    PPVID Entries Count                         : 0
        (None)

    VLAN Name Entries Count                     : 0
        (None)

    Protocol ID Entries Count                   : 0
        (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 Enabled:
            Capabilities                    : Not Support
            Network Policy                  : Not Support
            Location Identification         : Not Support
            Extended Power Via MDI          : Not Support
            Inventory                       : Not Support


    Inventory Management:
        None


Switch#
```

This example shows how to display normal LLDP information about neighboring devices connected to port 1.

```
Switch#show lldp neighbors interface eth1/0/1

Port ID: eth1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 80-26-89-15-28-A0
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/1
    Port Description                        :
    System Name                             :
    System Description                      :
    System Capabilities                     :
    Management Address Count                : 0
    Port PVID                               : 0
    PPVID Entries Count                     : 0
    VLAN Name Entries Count                 : 0
    Protocol ID Entries Count               : 0
    MAC/PHY Configuration/Status            : (None)
    Power Via MDI                           : (None)
    Link Aggregation                        : (None)
    Maximum Frame Size                      : 0
    LLDP-MED capabilities                   : (See Detail)
    Extended power via MDI                  : (See Detail)
    Network policy                          : (See Detail)
    Inventory Management                    : (See Detail)
    Unknown TLVs Count                      : 0


Switch#
```

This example shows how to display brief LLDP information about neighboring devices connected to ports 1 to 2.

```
Switch#show lldp neighbors interface eth1/0/1-2 brief

Port ID: eth1/0/1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 80-26-89-15-28-A0
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/1
    Port Description                        :

Port ID: eth1/0/2
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
    Chassis ID Subtype                      : MAC Address
    Chassis ID                              : 80-26-89-A5-43-D0
    Port ID Subtype                         : Local
    Port ID                                 : eth1/0/22
    Port Description                        :


Switch#
```

54-25 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/Privileged EXEC 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  : 0D4H31M5S
Total Inserts     : 5
Total Deletes     : 0
Total Drops       : 0
Total Ageouts     : 1

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 that the remote data was received but 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.

54-26 show lldp traffic interface

This command is used to display the LLDP traffic information on the specific physical interface.

show lldp traffic interface *INTERFACE-ID* **[, | -]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 eth1/0/1

Port ID : eth1/0/1
-------------------------------------------
    Total Transmits     : 55
    Total Discards      : 0
    Total Errors        : 0
    Total Receives      : 38
    Total TLV Discards  : 0
    Total TLV Unknowns  : 0
    Total Ageouts       : 0


Switch#
```

Display Parameters

Total Transmits	The total number of LLDP packets transmitted on the port.
Total Discards	The total number of LLDP frames discarded on the port for any reason.
Total Errors	The number of invalid LLDP frames received on the port.
Total Receives	The total number of LLDP packets received on the port.
Total TLV Discards	The number of TLVs discarded.
Total TLV Unknowns	The total number of LLDP TLVs received on the port where the type value is in the reserved range, and not recognized.
Total Ageouts	The total number of times a complete remote data entry was deleted for the port because the Time to Live interval expired.

55. Loopback Detection (LBD) Commands

55-1 loopback-detection (Global)

This command is used to enable the loopback detection function globally. Use the **no** form of this command to disable the function globally.

loopback-detection [mode {port-based | vlan-based}]

no loopback-detection [mode]

Parameters

mode	(Optional) Specifies the detection mode.
port-based	(Optional) Specifies that loop detection will work in the port-based mode.
vlan-based	(Optional) Specifies that 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 on ports that are connected to users, and VLAN-based detection is used in trunk or hybrid ports when the partner switch does not support the loop detection function.

When port-based detection is enabled, 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 in the path, 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 on the port.

When VLAN-based detection is enabled, the port will periodically send VLAN-based LBD packets for each VLAN that the port has membership in and 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, packet transmitting and receiving will be temporarily stopped in 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 detection and the port is an untagged member of multiple VLANs, 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)#
```

55-2 loopback-detection (Interface)

This command is used to enable the loopback detection function for an interface. Use the **no** form of this command to disable the function for an interface.

loopback-detection

no loopback-detection

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to enable or disable the loopback detection function on an interface.

Example

This example shows how to enable the loopback detection function on port 1.

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

55-3 loopback-detection interval

This command is used to configure the timer interval. Use the **no** form of this command to revert to the default setting.

loopback-detection interval *SECONDS*

no loopback-detection interval

Parameters

SECONDS	Specifies the interval in seconds at which LBD packets are transmitted. The valid range is from 1 to 32767.

Default

By default, this value is 10 seconds.

Command Mode

Global Configuration Mode.

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)#
```

55-4 loopback-detection vlan

This command is used to configure the VLANs to be enabled for loop detection. Use the **no** form of this command to revert to the default setting.

loopback-detection vlan *VLAN-LIST*

no loopback-detection vlan *VLAN-LIST*

Parameters

VLAN-LIST	Specifies the VLAN identification number, numbers, or range of numbers to be matched. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.

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.

By default, LBD Control packets are sent out for all VLANs that the port is a member of. LBD Control packets are sent out for the VLAN that the port is a member of 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)#
```

55-5 show loopback-detection

This command is used to display the current loopback-detection control settings.

show loopback-detection [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 display the current loopback detection settings and status.

```
Switch#show loopback-detection

 Loop Detection       : Enabled
 Detection Mode       : port-based
 LBD enabled VLAN     : all VLANs
 Interval             : 20 seconds
 Action Mode          : Shutdown
 Address Type         : Multicast
 Function Version     : v4.07

 Interface         State       Result               Time Left (sec)
 --------------    --------    -----------------    ---------------
 eth1/0/1          Enabled     Normal               -
 eth1/0/2          Disabled    Normal               -
 eth1/0/3          Disabled    Normal               -
 eth1/0/4          Disabled    Normal               -
 eth1/0/5          Disabled    Normal               -
 eth1/0/6          Disabled    Normal               -
 eth1/0/7          Disabled    Normal               -
 eth1/0/8          Disabled    Normal               -
 eth1/0/9          Disabled    Normal               -
 eth1/0/10         Disabled    Normal               -
 eth1/0/11         Disabled    Normal               -
 eth1/0/12         Disabled    Normal               -
 eth1/0/13         Disabled    Normal               -
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

This example shows how to display the loopback detection status for port 1.

```
Switch#show loopback-detection interface eth1/0/1

 Interface         State       Result               Time Left (sec)
 --------------    --------    -----------------    ---------------
 eth1/0/1          Enabled     Normal               -

Switch#
```

Display Parameters

Interface	Indicates the port that has loopback detection enabled.
State	Indicates the port state.
Result	Indicates whether a loop is detected.
Time Left	The remaining time before being auto-recovered.

55-6 loopback-detection action

This command is used to configure the loopback-detection mode. Use the **no** form of this command to revert to the default setting.

loopback-detection action {shutdown | none}

no loopback-detection action

Parameters

shutdown	Specifies to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected.
none	Specifies not to shut down the port in the port-based mode or block traffic on the specific VLAN in the VLAN-based mode when a loop has been detected.

Default

By default, this mode is **shutdown**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the loopback-detection mode.

Example

This example shows how to configure the loopback-detection mode.

```
Switch#configure terminal
Switch(config)#loopback-detection action none
Switch(config)#
```

55-7 snmp-server enable traps loopback-detection

This command is used to enable the sending of SNMP notifications for loopback detection. Use the **no** form of this command to revert to the default setting.

snmp-server enable traps loopback-detection

no snmp-server enable traps loopback-detection

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications for loopback detection.

Example

This example shows how to enable the sending of SNMP notifications for loopback detection.

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

55-8 loopback-detection address-type

This command is used to configure the DA type of loopback-detection packets. Use the **no** form of this command to revert to the default setting.

loopback-detection address-type {multicast | broadcast}

no loopback-detection address-type

Parameters

multicast	Specifies to only send multicast LBD packets. The DA is CF-00-00-00-00-00.
broadcast	Specifies to only send broadcast LBD packets. The DA is FF-FF-FF-FF-FF-FF.

Default

By default, this mode is **multicast**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the DA type of loopback-detection packets.

Example

This example shows how to configure the DA type of loopback-detection packets to broadcast.

```
Switch#configure terminal
Switch(config)#loopback-detection address-type broadcast
Switch(config)#
```

56. Loopback Test Commands

56-1 loopback

This command is used to configure the loopback mode of the physical port interfaces and to start testing. Use the **no** form of this command to clear the loopback setting and stop testing.

loopback {internal | external} {mac | phy [copper | fiber]}

no loopback

Parameters

internal	Specifies the internal loopback mode. MAC or PHY is set to internal loopback, and the CPU begins to send packets continuously to the port. All packets sent by the CPU are looped back to it, and then CPU checks the received packets to determine whether the packet path between the CPU, and MAC or PHY is correct.
external	Specifies the external loopback mode. MAC or PHY is set to external loopback (line loopback) mode. Packets sent by external traffic generator are looped back at the MAC or PHY layer, and sent back to the external traffic generator. The external traffic generator can then check the received packets to determine whether the packet path between MAC or PHY, and the external traffic generator is correct.
mac	Specifies to loop back at the MAC layer.
phy	Specifies to loop back at the PHY layer.
copper	(Optional) Specifies to test medium to copper.
fiber	(Optional) Specifies to test medium to fiber.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical ports.

Example

This example shows how to configure port 1 to start loopback test in internal PHY copper mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#loopback internal phy copper

Success

Switch(config-if)#
```

56-2 show loopback result

This command is used to display the loopback result for all or specified physical ports.

show loopback result [interface *INTERFACE-ID* **[- | ,]]**

Parameters

INTERFACE-ID	(Optional) Specifies the physical port interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the loopback result for all or specified physical ports.

Example

This example shows how to display the loopback result for port 1.

```
Switch#show loopback result interface eth1/0/1

Port       Loopback     64B          512B         1024B        1536B
           Mode         Tx    Rx     Tx    Rx     Tx    Rx     Tx    Rx
---------  -----------  ----- -----  ----- -----  ----- -----  ----- -----
eth1/0/1   Int. copper  9     9      9     9      9     9      9     9

Loopback Test Result : Success

Switch#
```

57. MAC Authentication Commands

57-1 mac-auth system-auth-control

This command is used to enable MAC authentication globally. Use the **no** form of this 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)#
```

57-2 mac-auth enable

This command is used to enable MAC authentication on the specified interface. Use the **no** form of this 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mac-auth enable
Switch(config-if)#
```

57-3 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 revert 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. In the clear text form, this string can be up to 16 characters long. In the encrypted form, the string can be up to 44 characters long.

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)#
```

57-4 mac-auth username

This command is used to configure the username for local and RADIUS authentication. Use the **no** form of this command to revert to the default setting.

mac-auth username *STRING*

no mac-auth username

Parameters

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 to authenticate MAC address users. The username is used to authenticate via both the local database and remote servers. If the command is not configured, the username for authentication 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 user1
Switch(config)#
```

57-5 snmp-server enable traps mac-auth

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

snmp-server enable traps mac-auth

no snmp-server enable traps mac-auth

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

None.

Example

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

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

58. Mirror Commands

58-1 monitor session destination interface

This command is used to configure the destination interface for a monitor session, allowing packets on source ports to be monitored via a destination port. Use the **no** form of this command to remove the destination interface of the session.

monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

no monitor session *SESSION-NUMBER* **destination interface** *INTERFACE-ID*

Parameters

SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
INTERFACE-ID	Specifies the destination interface for the monitor session.

Default

None.

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.

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 from the remote site.

Example

This example shows how to create a port monitor session with the session number 1. It assigns the physical port 1 as the destination port and three physical source ports 2 to 4 as monitor source ports.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface eth1/0/1
Switch(config)#monitor session 1 source interface eth1/0/2-4
Switch(config)#
```

58-2 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 this command to remove the configuration of the RSPAN VLAN.

monitor session *SESSION-NUMBER* **destination remote vlan** *VLAN-ID* **interface** *INTERFACE-ID*

monitor session *SESSION-NUMBER* **destination remote vlan access-list** *ACCESS-LIST-NAME* **replace vlan** *VLAN-ID*

no monitor session *SESSION-NUMBER* **destination remote vlan [access-list** *ACCESS-LIST-NAME***]**

Parameters

SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
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.
access-list *ACCESS-LIST-NAME*	(Optional) Specifies the flow used to perform egress per flow RSPAN VLAN replacement. The flow will still be configured even if the access list does not exist.
replace vlan *VLAN-ID*	(Optional) Specifies the VLAN ID used to replace the RSPAN VLAN ID for the matched flow of packets transmitted out from the destination port on a RSPAN source switch. The valid range is from 1 to 4094.

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 a 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. An interface cannot be specified for the command to transmit the monitored packets for multiple RSPAN sessions.

A flow can be defined by specifying an access list to be matched against the packets monitored by the session. The RSPAN VLAN ID is used to tunnel these packets and will be replaced by the Replace VLAN ID. For an RSPAN source session, multiple VLAN replacement flows can be configured. For remote sessions, it is suggested that the RSPAN VLAN is configured for dedicated use to monitor traffic only.

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 port 6 and three source ports 2 to 4 to be monitored.

```
Switch#configure terminal
Switch(config)#monitor session 2 source interface eth1/0/2-4
Switch(config)#monitor session 2 destination remote vlan 100 interface eth1/0/6
Switch(config)#
```

58-3 monitor session source interface

This command is used to configure the source port of a monitor session. Use the **no** form of this command to remove a source port from the monitor session.

monitor session *SESSION-NUMBER* **source interface {***INTERFACE-ID* **[, | -] [both | rx | tx] | cpu rx}**

no monitor session *SESSION-NUMBER* **source interface {***INTERFACE-ID* **[, | -] | cpu rx}**

Parameters

SESSION-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
interface *INTERFACE-ID*	Specifies the source interface for a monitor session.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
both	(Optional) Specifies to monitor the packets transmitted and received on the port.
rx	(Optional) Specifies to monitor the packets received on the port.
tx	(Optional) Specifies to monitor the packets transmitted on the port.
cpu rx	Specifies the CPU receiving mirror. All packets received by the CPU are mirrored.

Default

None.

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. This is the same as specifying **both**.

Example

This example shows how to create a port monitor session with session number 1. It assigns the physical port 1 as the destination port and three source physical ports 2 to 4 as monitor source ports.

```
Switch#configure terminal
Switch(config)#monitor session 1 destination interface eth1/0/1
Switch(config)#monitor session 1 source interface ethe1/0/2-4
Switch(config)#
```

58-4 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-NUMBER	Specifies the session number for the monitor session. The valid range is 1 to 4.
ACCESS-LIST-NAME	Specifies the flow-based mirror. Only the ingress mirror is supported and only MAC, IP, or IPv6 access lists can be monitored. Even if the access list does not exist, the flow-based mirror can still be configured.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Only one access list can be monitored on a session at a time (One access list can include multiple flows). When an access list is monitored, the packet filtered by the access list that is applied to the hardware via the **access-group** or **vlan map** command will be monitored.

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 eth1/0/1
Switch(config)#monitor session 2 source acl MAC-Monitored-flow
Switch(config)#
```

58-5 monitor session source remote vlan

This command is used to configure the RSPAN VLAN for an RSPAN destination session. Use the **no** form of this command to remove the configuration.

monitor session *SESSION-NUMBER* **source remote vlan** *VLAN-ID*

no monitor session *SESSION-NUMBER* **source remote vlan**

Parameters

SESSION-NUMBER	Specifies the session number of the monitor session. The valid range is 1 to 4.
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 from the remote site. Use the **monitor session destination interface** command to configure the destination port to transmit the monitored packets to.

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 port 4 as the destination port. It also assigns VLAN 100 as the RSPAN VLAN. The monitored packets arrive at port 5 and will be transmitted out from port 4.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#remote-span
Switch(config-vlan)#exit
Switch(config)#interface eth1/0/5
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#exit
Switch(config)#interface eth1/0/4
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 eth1/0/4
Switch(config)#
```

58-6 monitor session source vlan

This command is used to configure VLANs for VLAN-based monitoring. Use the **no** form of this command to remove VLANs from VLAN-based monitoring.

monitor session *SESSION-NUMBER* **source vlan** *VLAN-ID* **[, | -] rx**

no monitor session *SESSION-NUMBER* **source vlan** *VLAN-ID* **[, | -]**

Parameters

SESSION-NUMBER	Specifies the session number of the monitor session. The valid range is 1 to 4.
VLAN-ID	Specifies the VLAN ID to be configured for VLAN-based monitoring. The valid range is from 1 to 4094.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
rx	Specifies to monitor the packets received on the VLAN.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

For a monitor session, multiple VLANs can be specified, but a VLAN cannot be configured as the source VLAN of multiple sessions. The VLAN-based monitor **rx** parameter will mirror all ingress packets on the specified VLAN ID.

Example

This example shows how to create a monitor session with session number 2. It assigns three VLANs (VLAN 2, VLAN 3 and VLAN 4) as monitor source VLANs.

```
Switch#configure terminal
Switch(config)#monitor session 2 destination interface eth1/0/1
Switch(config)#monitor session 2 source vlan 2-4 rx
Switch(config)#
```

58-7 remote-span

This command is used to specify a VLAN as an RSPAN VLAN. Use the **no** form of this command to revert to a non-RSPAN VLAN.

remote-span

no remote-span

Parameters

None.

Default

By default, 802.1Q VLAN is used.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command 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 any of the intermediate switches and the destination switch involved in the RSPAN session.

For any of the intermediate switches involved in a RSPAN session, the port that the monitored packets arrive on and the port that the monitored packets leave from 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 on an intermediate switch in the RSPAN session. Port 1 is where the monitored packets arrive on and port 5 is where the monitored packets leave.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan 100
Switch(config-if)#exit
Switch(config)#interface eth1/0/5
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)#
```

58-8 no monitor session

This command is used to delete a monitor session.

no monitor session *SESSION-NUMBER*

Parameters

SESSION-NUMBER	Specifies the session number of the monitor session to be deleted. The valid range is from 1 to 4.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If a monitor session is deleted, all configuration for the session is removed.

Example

This example shows how to delete the monitor session with session number 1.

```
Switch#configure terminal
Switch(config)#no monitor session 1
Switch(config)#
```

58-9 show monitor session

This command is used to display all or a specific monitor 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/Privileged EXEC 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 port monitor session with the session number 1.

```
Switch#show monitor session

 Session 1
     Session Type: local session
     Destination Port: Ethernet1/0/1
     Source Ports:
         Both:
             Ethernet1/0/2
             Ethernet1/0/3
             Ethernet1/0/4

 Total Entries: 1

Switch#
```

59. Multicast Listener Discovery (MLD) Commands

59-1 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 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)#
```

59-2 ipv6 mld last-listener-query-count

This command is used to configure the number of group-specific or group-and-source-specific queries sent before the router assumes there are no local members of a group. Use the **no** form of this 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

The user can use this command to configure the number of group-specific or group-and-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 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)#
```

59-3 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 this 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 between group-specific or group-and-source-specific queries, in seconds. 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

When an MLD querier receives a packet to leave the specific group or channel, it will send a group-specific or group-and-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, the interface's

membership will be removed from the group or channel that is to be left. The value of the leave timer is calculated as follows: (last listener query interval) x (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)#
```

59-4 ipv6 mld query-interval

This command is used to configure the interval at which the router sends MLD general query messages. Use the **no** form of this 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 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 to 150 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld query-interval 150
Switch(config-if)#
```

59-5 ipv6 mld query-max-response-time

This command is used to configure the maximum response time advertised in MLD queries. Use the **no** form of this command to revert to the default setting.

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

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 maximum response time for VLAN 1000. It configures the MLD query maximum response time to 10 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld query-max-response-time 10
Switch(config-if)#
```

59-6 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 setting.

ipv6 mld robustness-variable *VALUE*

no ipv6 mld robustness-variable

Parameters

VALUE	Specifies the robustness variable. The valid value range is 1 to 7.

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 MLD 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).

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)#
```

59-7 ipv6 mld version

This command is used to change the MLD version on the specified interface. Use the **no** form of this command to revert to the default setting.

ipv6 mld version *NUMBER*

no ipv6 mld version

Parameters

NUMBER	Specifies the MLD version. **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 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)#
```

59-8 ipv6 mld static-group

This command is used to create a static membership on an interface for a group or channel. Use the **no** form of this command to delete the membership.

ipv6 mld static-group *GROUP-ADDRESS*

no ipv6 mld static-group *GROUP-ADDRESS*

Parameters

GROUP-ADDRESS	Specifies an IPv6 multicast group address.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an MLD static group in case the attached host does not support MLD protocol.

Example

This example shows how to create an MLD static group on VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface vlan1000
Switch(config-if)#ipv6 mld static-group FF1E::1
Switch(config-if)#
```

59-9 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 | static}]**

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.
static	(Optional) Specifies to display the static group information.

Default

None.

Command Mode

User/Privileged EXEC 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
------------------------------------------------------------------
FF12::1:FF00:65                     vlan1      0DT00H05M26S 0DT00H01M12S
FF12::1:FF23:86CC                   vlan1      0DT00H03M26S 0DT00H01M55S
FF12::4:FF00:1                      vlan1      0DT00H04M12S Stopped
Total Entries: 3

Switch#
```

This example shows how to display MLD group detailed information of group ff12::1:ff23:86cc.

```
Switch#show ipv6 mld groups ff12::1:ff23:86cc detail

Interface      : vlan1
Group          : FF12::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#
```

This example shows how to display MLD static group information.

```
Switch#show ipv6 mld groups static

Interface        Multicast Group
------------     ---------------
vlan1000         FF1E::1

Total Entries: 1

Switch#
```

Display Parameters

Uptime	The time elapsed since the entry has been created, in the format: [n]DT[n]H[n]M[n]S.
Expires	The time that the entry will be removed if the entry is not refreshed, in the format: [n]DT[n]H[n]M[n]S. **Stopped:** Indicates that the timeout of this entry is not determined by the expire timer. If the router is in Include mode for a group, the whole group entry will time out after the last source entry times out (unless the mode is changed to Exclude mode before it times out). **Static:** Indicates that the entry is created manually and timing out of this entry is not determined by this expire timer.
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.

59-10 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/Privileged EXEC 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:FE86:5649/128
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

Total Entries: 1

Switch#
```

Display Parameters

Version	The MLD protocol version running on the interface.
Querier	The querier IP on the interface LAN.

60. Multicast Listener Discovery (MLD) Proxy Commands

60-1 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 works in a simple tree topology. Make sure there are no other multicast routers except for the proxy 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)#
```

60-2 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)#
```

60-3 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 an IPv6 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)#
```

60-4 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 this option.

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 IPv6 address configured and is set as the downstream interface.

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 a forwarder. Use the configuration in the appropriate topology. Improper usage may cause local loops or redundant traffic.

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)#
```

60-5 show ipv6 mld proxy

This command is used to display the MLD proxy configuration.

show ipv6 mld proxy

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the upstream interface configuration and downstream interfaces.

Example

This example shows how to display the MLD proxy configuration on the Switch.

```
Switch#show ipv6 mld proxy

MLD Proxy Global State:    Enabled
Upstream Interface:        vlan14
Downstream Interface:
vlan11, vlan12(DF), vlan13(DF)

Switch#
```

60-6 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display multicast groups learned by the MLD proxy function. If no optional parameter is specified, all group information will be displayed.

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 for 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#
```

60-7 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/Privileged EXEC 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#
```

61. Multicast Listener Discovery (MLD) Snooping Commands

61-1 clear ipv6 mld snooping statistics

This command is used to clear MLD snooping statistic counters on 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 a VLAN to clear the IPv6 MLD snooping statistics.
interface *INTERFACE-ID*	Specifies a port to clear the IPv6 MLD snooping statistics.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear MLD snooping statistic counters on the Switch.

Example

This example shows how to clear all MLD snooping statistics.

```
Switch#clear ipv6 mld snooping statistics all
Switch#
```

61-2 ipv6 mld snooping

This command is used to enable MLD snooping. Use the **no** form of this command to disable MLD snooping.

ipv6 mld snooping

no ipv6 mld snooping

Parameters

None.

Default

MLD snooping is disabled on all VLANs.

The MLD snooping global state is disabled by default.

Command Mode

Global Configuration Mode.

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This function must be enabled in both Global Configuration Mode and VLAN Configuration Mode for a VLAN to operate with MLD snooping. IGMP snooping and MLD snooping can be simultaneously enabled on the same VLAN.

Example

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)#
```

61-3 ipv6 mld snooping access-group

This command is used to restrict the receivers on a subnet to only join the multicast groups that are permitted in a standard IPv6 access list. Use the **no** form of this command to disable this function.

ipv6 mld snooping access-group *IPV6-ACCESS-LIST-NAME* **[vlan** *VLAN-ID***]**

no ipv6 mld snooping access-group [vlan *VLAN-ID***]**

Parameters

IPV6-ACCESS-LIST-NAME	Specifies a standard IPv6 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 *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN and applies the filter to packets that arrive on the VLAN.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to restrict the multicast traffic receiver to join to a specific group. The destination address in the access list represents the multicast group address that is used to permit the receiver to join the multicast group or to deny the receiver from joining the multicast group.

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

Example

This example shows how to restrict the serviced MLD snooping group to FF1E::14 on port 1. In the following example, first, create an IPv6 access list named “mld_filter” which only permits the packets destined for the group address FF1E::14. Then, associate this access group with port 1.

```
Switch#configure terminal
Switch(config)#ipv6 access-list mld_filter
Switch(config-ipv6-acl)#permit any host FF1E::14
Switch(config-ipv6-acl)#end
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 mld snooping access-group mld_filter
Switch(config-if)#
```

61-4 ipv6 mld snooping fast-leave

This command is used to configure MLD snooping fast-leave on the interface. Use the **no** form of this 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

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to allow MLD membership to be removed from a port immediately after receiving the leave message without using the group-specific or group-and-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)#
```

61-5 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 this command to revert to the default setting.

ipv6 mld snooping last-listener-query-interval *SECONDS*

no ipv6 mld snooping last-listener-query-interval

Parameters

SECONDS	Specifies the maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. The range of this value is 1 to 25.

Default

By default, this value is 1 second.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

On receiving a 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)#
```

61-6 ipv6 mld snooping limit

This command is used to set the limit of MLD snooping multicast groups or channels which layer 2 interface can join. Use the **no** form of this command to remove the limitation.

ipv6 mld snooping limit *NUMBER* **[exceed-action {drop | replace}] [except** *IPv6-ACCESS-LIST-NAME***] [vlan** *VLAN-ID***]**

no ipv6 mld snooping limit [vlan *VLAN-ID***]**

Parameters

NUMBER	Specifies the maximum number of MLD snooping groups that the interface can join. This value must between 1 and 256.
exceed-action	(Optional) Specifies the action for handling newly learned groups when the limitation is exceeded.
drop	(Optional) Specifies that the new group will be dropped.
replace	(Optional) Specifies that the new group will replace the oldest group.
except *IPv6-ACCESS-LIST-NAME*	(Optional) Specifies a standard IPv6 access list. The group (*,G) or channel (S,G) permitted in the access list will be excluded from the limit. To permit a channel (S,G), S is specified in the source address field and G is specified in the destination address field of the access list entry. To permit a group (*,G), “any” is specified in the source address field and G is specified in the destination address field of the access list entry.
vlan *VLAN-ID*	(Optional) Specifies a Layer 2 VLAN 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.

Example

This example shows how to set the limit of MLD snooping groups that VLAN ID 1000 on port 4 can join and specify the “mld_filter” access list to be excluded from the limit.

```
Switch#configure terminal
Switch(config)#interface eth1/0/4
Switch(config-if)#ipv6 mld snooping limit 80 except mld_filter vlan 1000
Switch(config-if)#
```

This example shows how to remove the limit of MLD snooping groups that port-channel 4 with VLAN ID 1000 can join.

```
Switch#configure terminal
Switch(config)#interface port-channel 4
Switch(config-if)#no ipv6 mld snooping limit vlan 1000
Switch(config-if)#
```

61-7 ipv6 mld snooping mrouter

This command is used to configure the specified interface(s) as router ports or ports forbidden from becoming 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 not being connected to multicast-enabled routers.
INTERFACE-ID	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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
learn pimv6	Specifies to enable dynamic learning on multicast router ports.

Default

No IPv6 MLD snooping multicast router port is configured.

Auto-learning is enabled.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To specify a multicast router port, the valid interface can be a physical port or a port-channel. The specified multicast router port must be the 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 packets to identify whether the partner device is a router.

Example

This example shows how to configure port 1 as an MLD snooping multicast router port and port 2 as an MLD snooping forbidden multicast router port on VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ipv6 mld snooping mrouter interface eth1/0/1
Switch(config-vlan)#ipv6 mld snooping mrouter forbidden interface eth1/0/2
Switch(config-vlan)#
```

This example shows how to 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)#
```

61-8 ipv6 mld snooping ignore-topology-change-notification

This command is used to make MLD snooping ignore STP changes and not send an STP triggered query on the interface. Use the **no** form of this command to make MLD snooping aware 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

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

An MLD snooping switch is aware of link-layer topology changes caused by Spanning Tree operation. When a port is enabled or disabled by 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 ignore the topology changes.

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)#
```

61-9 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

source *IPV6-ADDRESS*	(Optional) Specifies the source IP address of proxy reporting.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The proxy reporting function only works for MLDv1 traffic.

When the proxy reporting function is enabled, the received multiple MLD report or leave packets are integrated into one report before being sent to the router port. The proxy reporting source IP will be used as source IP of the report, and the 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, 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)#
```

61-10 ipv6 mld snooping querier

This command is used to enable the MLD snooping querier on the Switch. Use the **no** form of this command to disable the MLD snooping querier function.

ipv6 mld snooping querier

no ipv6 mld snooping querier

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the system can play the querier role, the entity will listen for MLD query packets sent by other devices. If an MLD query message is received, the device with lower IPv6 address becomes the querier. If the MLD protocol is also enabled on the interface, the 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)#
```

61-11 ipv6 mld snooping query-interval

This command is used to configure the interval at which the MLD snooping querier sends MLD general query messages. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping query-interval *SECONDS*

no ipv6 mld snooping query-interval

Parameters

SECONDS	Specifies the interval at which the designated router sends MLD general query messages. The range is 1 to 31744.

Default

By default, this value is 125 seconds.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The query interval is the interval between general queries sent by the querier. By varying the query interval, an administrator may tune the number of MLD messages on the network. Larger values cause MLD Queries to be sent less often.

Example

This example shows how to configure the MLD snooping query interval to 300 seconds on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-interval 300
Switch(config-vlan)#
```

61-12 ipv6 mld snooping query-max-response-time

This command is used to configure the maximum response time advertised in MLD snooping queries. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping query-max-response-time *SECONDS*

no ipv6 mld snooping query-max-response-time

Parameters

SECONDS	Specifies to set the maximum response time, in seconds, advertised in MLD snooping queries. The range is from 1 to 25.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the period of which the group member can respond to an MLD query message before the MLD Snooping deletes the membership.

Example

This example shows how to configure the maximum response time to 20 seconds on an interface.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-max-response-time 20
Switch(config-vlan)#
```

61-13 ipv6 mld snooping query-version

This command is used to configure the general query packet version sent by the MLD snooping querier. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping query-version *NUMBER*

no ipv6 mld snooping query-version

Parameters

NUMBER	Specifies that the version of the MLD general query sent by MLD snooping querier. The value is 1 and 2.

Default

By default, the version number is 2.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the general query packet version sent by the MLD snooping querier.

Example

This example shows how to configure the query version to be 1 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping query-version 1
Switch(config-vlan)#
```

61-14 ipv6 mld snooping rate-limit

This command is used to configure the upper limit of ingress MLD control packets per second. 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. The value is from 1 to 1000.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In the Interface Configuration Mode, this command is only available for physical port and port-channel interface configuration.

Use this command to configure the upper limit of ingress MLD control packets per second.

Example

This example shows how to limit 30 packets per second on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ipv6 mld snooping rate-limit 30
Switch(config-if)#
```

This example shows how to limit 30 packets per second on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping rate-limit 30
Switch(config-vlan)#
```

61-15 ipv6 mld snooping report-suppression

This command is used to enable MLD report suppression on a VLAN. Use the **no** form of this command to disable report suppression on a VLAN.

ipv6 mld snooping report-suppression

no ipv6 mld snooping report-suppression

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The report suppression function only works for MLDv1 traffic.

When report suppression is enabled, the Switch suppresses duplicate reports sent by hosts. Suppression for the same group report or leave messages will continue until the suppression time expires. For report or leave messages to the same group, only one report or leave message is forwarded. The remaining report and leave messages are suppressed.

Example

This example shows how to enable MLD report suppression.

```
Switch#configure terminal
Switch(config)#vlan 100
Switch(config-vlan)#ipv6 mld snooping report-suppression
Switch(config-vlan)#
```

61-16 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 setting.

ipv6 mld snooping robustness-variable *VALUE*

no ipv6 mld snooping robustness-variable

Parameters

VALUE	Specifies the robustness variable. The value is from 1 to 7.

Default

By default, this value is 2.

Command Mode

VLAN 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 MLD 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.

This value can be increased if a subnet is expected to lose packets.

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)#
```

61-17 ipv6 mld snooping static-group

This command is used to configure an MLD snooping static group. Use the **no** form of this command to delete a static group.

ipv6 mld snooping static-group *IPV6-ADDRESS* **interface** *INTERFACE-ID* **[, | -]**

no ipv6 mld snooping static-group *IPV6-ADDRESS* **[interface** *INTERFACE-ID* **[, | -]]**

Parameters

IPV6-ADDRESS	Specifies an IPv6 multicast group address.
interface *INTERFACE-ID*	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No static-group is configured.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command applies to MLD snooping on a VLAN to statically add group membership entries and/or source records.

Use this command to create an MLD snooping static group in case that the attached host does not support the 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 eth1/0/5
Switch(config-vlan)#
```

61-18 ipv6 mld snooping suppression-time

This command is used to configure the time for suppressing duplicate MLD reports or leaves. Use the **no** form of this command to revert to the default setting.

ipv6 mld snooping suppression-time *SECONDS*

no ipv6 mld snooping suppression-time

Parameters

SECONDS	Specifies to configure the time for suppressing duplicates MLD reports. The range is 1 to 300.

Default

By default, this value is 10 seconds.

Command Mode

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Report suppression will suppress the duplicate MLD report or leave packets received in the suppression time. A small suppression time will cause the duplicate MLD packets be sent more frequently.

Example

This example shows how to configure the suppression time to be 125 on VLAN 1000.

```
Switch#configure terminal
Switch(config)#vlan 1000
Switch(config-vlan)#ipv6 mld snooping suppression-time 125
Switch(config-vlan)#
```

61-19 ipv6 mld snooping minimum-version

This command is used to configure the minimum version of 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

VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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)#
```

61-20 show ipv6 mld snooping

This command is used to display MLD snooping information on the Switch.

show ipv6 mld snooping [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no optional parameter is specified, MLD snooping information for all VLANs with MLD snooping enabled will be displayed.

Example

This example shows how to display MLD snooping configuration.

```
Switch#show ipv6 mld snooping

MLD snooping global state: Enabled

VLAN #1 configuration
    MLD snooping state           : Enabled
    Minimum version              : v1
    Fast leave                   : Disabled (host-based)
    Report suppression           : Disabled
    Suppression time             : 10 seconds
    Proxy reporting              : Disabled (Source ::)
    Mrouter port learning        : Enabled
    Querier state                : Disabled
    Query version                : v2
    Query interval               : 125 seconds
    Max response time            : 10 seconds
    Robustness value             : 2
    Last listener query interval : 1 seconds
    Rate limit                   : 0
    Ignore topology change       : Disabled

Total Entries: 1

Switch#
```

61-21 show ipv6 mld snooping filter

This command is used to display MLD snooping filter information for specified interface(s).

show ipv6 mld snooping filter [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces to be displayed. The interface can be a physical interface or a port-channel.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MLD snooping limit and access group information. If no optional parameter is specified, MLD snooping filter information for all interfaces will be displayed.

Example

This example shows how to display filter information when no interface is specified.

```
Switch#show ipv6 mld snooping filter

eth1/0/1:
    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)

eth1/0/3:
    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#
```

61-22 show ipv6 mld snooping groups

This command is used to display MLD snooping dynamic group information learned on the Switch.

show ipv6 mld snooping groups [*IPV6-ADDRESS* **| vlan** *VLAN-ID***] [detail]**

Parameters

IPV6-ADDRESS	(Optional) Specifies the group IP address. If no IPv6 address is specified, all MLD group information will be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD group information about all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
detail	(Optional) Specifies to display the MLD group detail information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MLD dynamic group information by command.

Example

This example shows how to display MLD snooping dynamic group information.

```
Switch#show ipv6 mld snooping groups

Total Group Entries : 1
Total Source Entries: 1

vlan1, FF1E::1
Learned on port: 1/0/3

Switch#
```

61-23 show ipv6 mld snooping mrouter

This command is used to display MLD snooping multicast router information that has been automatically learned and manually configured on the Switch.

show ipv6 mld snooping mrouter [vlan *VLAN-ID* **[, | -]]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed. If no VLAN is specified, MLD snooping Multicast Router Information on all VLANs will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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         1/0/3, 1/0/4   (static)
           1/0/6   (forbidden)
           1/0/7   (dynamic)

3         1/0/8   (static)
           1/0/9   (dynamic)

Total Entries: 2

Switch#
```

61-24 show ipv6 mld snooping static-group

This command is used to display statically configured MLD snooping groups on the Switch.

show ipv6 mld snooping static-group [*GROUP-ADDRESS* **| vlan** *VLAN-ID***]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group IPv6 address to be displayed.
vlan *VLAN-ID*	(Optional) Specifies the VLAN ID to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display statically configured MLD snooping groups on the Switch. If no optional parameter is specified, all information will be displayed.

Example

This example shows how to display statically configured MLD snooping groups.

```
Switch#show ipv6 mld snooping static-group

VLAN ID Group address                              Interface
------- ---------------------------------------- ------------------
1       FF1E::1                                  1/0/1-1/0/2

Total Entries: 1

Switch#
```

61-25 show ipv6 mld snooping statistics

This command is used to display MLD snooping statistics information on the Switch.

show ipv6 mld snooping statistics {interface [*INTERFACE-ID***[, | -]] | vlan [***VLAN-ID* **[, | -]]}**

Parameters

interface	Specifies to display statistics counters by interface.
INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan	Specifies to display statistics counters by VLAN.
VLAN-ID	(Optional) Specifies the VLAN ID to be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 on ports 4, 7 and 9.

```
Switch#show ipv6 mld snooping statistics interface eth1/0/4,1/0/7,1/0/9

Interface eth1/0/4
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth1/0/7
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0

Interface eth1/0/9
  Rx: v1Report 0, v2Report 0, Query 0, v1Done 0
  Tx: v1Report 0, v2Report 0, Query 0, v1Done 0


Total Entries: 3

Switch#
```

This example shows how to display MLD snooping statistics information of VLAN 20.

```
Switch#show ipv6 mld snooping statistics vlan 20

VLAN 20 Statistics:
  Rx: v1Report 0, v2Report 0, Query 953, v1Done 0
  Tx: v1Report 667, v2Report 1, Query 996, v1Done 0

Total Entries: 1

Switch#
```

62. Multicast Source Discovery Protocol (MSDP) Commands

62-1 ip msdp

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

ip msdp

no ip msdp

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

None.

Example

This example shows how to enable the MSDP function.

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

62-2 ip msdp connect-retry-interval

This command is used to configure the interval between attempts to re-establish a peering session after the MSDP peering session has been reset. Use the **no** form of this command to revert to the default setting.

ip msdp connect-retry-interval *SECONDS*

no ip msdp connect-retry-interval

Parameters

SECONDS	Specifies the connect retry time interval in seconds. The range is from 1 to 65535.

Default

By default, this value is 30 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A larger connect retry time interval delays the time between attempts to re-establish the peer session. For best results, configure the value in the range from 1 to 60 seconds.

Example

This example shows how to configure the connect retry interval to 50 seconds.

```
Switch#configure terminal
Switch(config)#ip msdp connect-retry-interval 50
Switch(config)#
```

62-3 ip msdp sa-originating-filter

This command is used to configure the Source-Active (SA) origination filter. Use the **no** command to revert this to the default setting.

ip msdp sa-originating-filter [list *ACCESS-LIST-NAME***]**

no ip msdp sa-originating-filter

Parameters

list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the standard IP access list that defines (S, G) pairs.

Default

By default, the SA message originating filter is not configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

A Rendezvous Point (RP) is configured to run MSDP and originates SA messages for all local sources that register with the RP. If no optional parameter is specified, an RP originating SA messages for all local sources can be prevented.

When configuring **ip msdp sa-originating-filter** with a list, an RP will only originate SA messages for local sources by sending to specified groups that match (S, G) pairs defined in a standard IP access list.

Example

This example shows how to configure the SA message origination filter.

```
Switch#configure terminal
Switch(config)#ip msdp sa-originating-filter list source1
Switch(config)#
```

62-4 ip msdp sa-cache-time

This command is used to configure the expiry time for SA cache entries. Use the **no** form of this command to revert to the default setting.

ip msdp sa-cache-time *SECONDS*

no ip msdp sa-cache-time

Parameters

SECONDS	Specifies the expiry time for SA cache entries in seconds. The range is from 65 to 65535 seconds.

Default

By default, this value is 145 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The interval for originating SA messages is 60 seconds and cannot be modified, so the SA cache expiry time can be tuned to allow for the expected packet loss on the network.

Example

This example shows how to configure the expiry time for SA cache.

```
Switch#configure terminal
Switch(config)#ip msdp sa-cache-time 210
Switch(config)#
```

62-5 ip msdp peer

This command is used to create an MSDP peer. Use the **no** form of this command to delete an MSDP peer.

ip msdp peer *PEER-ADDRESS* **connect-interface** *INTERFACE-ID*

no ip msdp peer *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
connect-interface *INTERFACE-ID*	Specifies the local interface that is used as the source IP address for TCP connections.

Default

By default, no MSDP peer exists.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The MSDP peer is specified by IP address.

Example

This example shows how to create an MSDP peer on interface VLAN 1.

```
Switch#configure terminal
Switch(config)#ip msdp peer 10.1.1.1 connect-interface vlan1
Switch(config)#
```

62-6 ip msdp peer description

This command is used to configure a description for an MSDP peer to make it easier to identify. Use the **no** form of this command to delete the description.

ip msdp peer description *PEER-ADDRESS STRING*

no ip msdp peer description *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
STRING	Specifies the description of the MSDP peer.

Default

By default, there is no description for the MSDP peer.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The description must be configured for an existing MSDP peer.

Example

This example shows how to configure the description for the peer 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip msdp peer description 10.1.1.1 router a
Switch(config)#
```

62-7 ip msdp peer shutdown

This command is used to shut down the TCP connection between two peers. Use the **no** form of this command to configure the MSDP peer to the **no shutdown** state.

ip msdp peer shutdown *PEER-ADDRESS*

no ip msdp peer shutdown *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.

Default

By default, the MSDP peer is in the **no shutdown** state.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The shutdown state must be configured on an existing MSDP peer. If the MSDP peer is in the shutdown state, the TCP connection between two peers will not be established. If the MSDP peer is in the no shutdown state, the TCP connection between two peers will attempt to re-establish.

Example

This example shows how to shut down the peer 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip msdp peer shutdown 10.1.1.1
Switch(config)#
```

62-8 ip msdp peer password

This command is used to enable MD5 password encryption for TCP connections between two peers. Use the **no** form of this command to disable MD5 password encryption.

ip msdp peer password *PEER-ADDRESS PASSWORD*

no ip msdp peer password *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
PASSWORD	Specifies the MD5 password.

Default

By default, the MD5 password encryption is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

MD5 authentication must be configured with the same password on both MSDP peers. Otherwise, the connection between them cannot be established.

Example

This example shows how to enable MD5 encryption for MSDP peer 10.1.1.1.

```
Switch#configure terminal
Switch(config)#ip msdp peer password 10.1.1.1 testmd5
Switch(config)#
```

62-9 ip msdp peer keep-alive

This command is used to configure the interval at which an MSDP peer sends keep-alive messages. Use the **no** form of this command to revert to the default setting.

ip msdp peer keep-alive *PEER-ADDRESS* **{***SECONDS* **| infinity}**

no ip msdp peer keep-alive *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
SECONDS	Specifies the keep-alive interval of the MSDP peer in seconds. The range is from 1 to 21845.
infinity	Specifies the MSDP peer to never send keep-alive messages.

Default

By default, the keep-alive interval is 60 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The keep-alive interval should be less than the hold time configured on the remote side of the MSDP TCP connection, otherwise the remote side of MSDP TCP connection may be disconnected before receiving the MSDP keep-alive message.

Example

This example shows how to configure the keep-alive interval to 50.

```
Switch#configure terminal
Switch(config)#ip msdp peer keep-alive 10.1.1.1 50
Switch(config)#
```

62-10 ip msdp peer hold-time

This command is used to configure the interval at which an MSDP peer will wait for keep-alive messages from other peers before declaring them as down. Use the **no** form of this command to revert to the default setting.

ip msdp peer hold-time *PEER-ADDRESS* **{***SECONDS* **| infinity}**

no ip msdp peer hold-time *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
SECONDS	Specifies the hold-time interval of the MSDP peer in seconds. The range is from 3 to 65535.
infinity	Specifies that the connection between two peers is never torn down.

Default

By default, the hold time interval is 75 seconds.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The hold-time interval must be larger than keep-alive time configured on the remote side of the MSDP TCP connection. Otherwise the MSDP TCP connection may be disconnected before receiving the MSDP keep-alive message.

Example

This example shows how to configure the hold time interval to 60.

```
Switch#configure terminal
Switch(config)#ip msdp peer hold-time 10.1.1.1 60
Switch(config)#
```

62-11 ip msdp peer sa-filter-in

This command is used to control the SA messages received from a peer. Use the **no** form of this command to revert to the default setting.

ip msdp peer sa-filter-in *PEER-ADDRESS* **[list** *ACCESS-LIST-NAME***]**

no ip msdp peer sa-filter-in *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the standard IP access list that defines (S, G) pairs.

Default

By default, the SA message incoming filter is not configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The router will receive all SA messages sent to it from the specified peer. By configuring **ip msdp sa-filter-in** without any access list, the router will ignore all SA messages sent to it from the specified peer. By configuring **ip msdp sa-filter-in** with a list, the router will only receive incoming SA messages from the specified peer that matches the (S, G) pairs defined in standard IP access list.

Example

This example shows how to configure the SA message incoming filter.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-filter-in 10.1.1.1 list msdp_in
Switch(config)#
```

62-12 ip msdp peer sa-filter-out

This command is used to control the SA messages that forward to a peer. Use the **no** form of this command to revert to the default setting.

ip msdp peer sa-filter-out *PEER-ADDRESS* **[list** *ACCESS-LIST-NAME***]**

no ip msdp peer sa-filter-out *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the standard IP access list that defines (S, G) pairs.

Default

By default, the SA message outgoing filter is not configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The router will forward all SA messages to an MSDP peer. By configuring **ip msdp sa-filter-out** without any access list, the router will stop forwarding SA messages to the specified peer. By configuring **ip msdp sa-filter-out** with a list, the router only forwards SA messages that match (S, G) pairs defined in the standard IP access list to the specified peer.

Example

This example shows how to configure the SA outgoing filter.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-filter-out 10.1.1.1 list msdp_out
Switch(config)#
```

62-13 ip msdp peer sa-filter-request

This command is used to control the SA request messages that a router will process from a specified peer. Use the **no** form of this command to revert to the default setting.

ip msdp peer sa-filter-request *PEER-ADDRESS* **[list** *ACCESS-LIST-NAME***]**

no ip msdp peer sa-filter-request *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the standard IP access list that defines the group.

Default

By default, the SA request message filter is not configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The router will process all SA request messages from the specified peer. By configuring **ip msdp sa-filter-request** without any access list, the router will stop processing SA request messages from the specified peer. By configuring **ip msdp sa-filter-request** with a list, the router only processes SA request messages in request groups that are defined in the standard IP access list from the specified peer.

Example

This example shows how to configure the SA request message filter.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-filter-request 10.1.1.1
Switch(config)#
```

62-14 ip msdp peer minimum-ttl

This command is used to specify a minimum TTL value for data-encapsulated SA messages sent to the specified MSDP peer. Use the **no** form of this command to revert to the default setting.

ip msdp peer minimum-ttl *PEER-ADDRESS TTL*

no ip msdp peer minimum-ttl *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
TTL	Specifies the minimum TTL value for data-encapsulated SA messages sent to specified MSDP peers. The range is from 0 to 255.

Default

By default, this value is 0.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When an SA message is sent from an MSDP peer, the TTL is decreased. If the TTL is smaller than the minimum TTL value of the MSDP peer that the SA message is sent to, the SA message will not be sent out.

Example

This example shows how to configure the minimum TTL value.

```
Switch#configure terminal
Switch(config)#ip msdp peer minimum-ttl 10.1.1.1 100
Switch(config)#
```

62-15 ip msdp peer sa-cache-maximum

This command is used to configure the maximum number of SA cache entries learned from the peer. Use the **no** form of this command to revert to the default setting.

ip msdp peer sa-cache-maximum *PEER-ADDRESS* **{***COUNT* **| none** }

no ip msdp peer sa-cache-maximum *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
COUNT	Specifies the maximum number of SA cache entries learned from the peer. The range is form 0 to 256.
none	Specifies that no limitation is applied for the number of SA cache entries.

Default

By default, the maximum number of SA cache entries is **none**.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the maximum number of SA cache entries is configured to zero, the Switch cannot learn SA cache entries from the peer. When the existing SA cache entries reach the maximum number of SA cache entries, the older SA cache entries will be removed until the number of SA cache entries is equal to the specified maximum number.

Example

This example shows how to configure the maximum number of SA cache entries to 10.

```
Switch#configure terminal
Switch(config)#ip msdp peer sa-cache-maximum 10.1.1.1 10
Switch(config)#
```

62-16 ip msdp static-rpf

This command is used to configure a default MSDP peer from which to accept all MSDP messages. Use the **no** form of this command to remove the static RPF configuration.

ip msdp static-rpf *PEER-ADDRESS* **[rp-list** *ACCESS-LIST-NAME***]**

no ip msdp static-rpf *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
rp-list *ACCESS-LIST-NAME*	(Optional) Specifies the name of the standard IP access list that defines the RP prefix list.

Default

By default, a static RPF peer is not defined.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Before configuring a static RPF peer, an MSDP peer must be added first by using the **ip msdp peer** command. If the RP prefix list is specified, the peer will be a static RPF peer only for RPs in the prefix list. When multiple static RPF peers are specified without an RP prefix list, only the connected peer whose address is lowest will be the active static RPF peer. If an MSDP peer is configured as a static RPF peer multiple times, only the last configuration entry takes effect. If there is one MSDP peer only, this MSDP peer works as a static RPF peer.

Example

This example shows how to configure an MSDP peer 10.1.1.1 as the static RPF peer.

```
Switch#configure terminal
Switch(config)#ip msdp static-rpf 10.1.1.1 rp-list rplist1
Switch(config)#
```

62-17 ip msdp mesh-group

This command is used to add an MSDP peer to the specified mesh group. Use the **no** form of this command to remove an MSDP peer from the mesh group.

ip msdp mesh-group *PEER-ADDRESS MESH-NAME*

no ip msdp mesh-group *PEER-ADDRESS*

Parameters

PEER-ADDRESS	Specifies the MSDP peer IP address.
MESH-NAME	Specifies the name of the mesh group.

Default

By default, the mesh group is not defined.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Before adding an MSDP peer to the mesh group, an MSDP peer must be added first using the **ip msdp peer** command. If an MSDP peer has been added to multiple mesh groups, only the last configuration entry takes effect.

Example

This example shows how to add the MSDP peer 10.1.1.1 to the mesh group “mesh1”.

```
Switch#configure terminal
Switch(config)#ip msdp mesh-group 10.1.1.1 mesh1
Switch(config)#
```

62-18 clear ip msdp peer

This command is used to clear the TCP connection to the specified MSDP peer.

clear ip msdp peer [*PEER-ADDRESS***]**

Parameters

PEER-ADDRESS	(Optional) Specifies the MSDP peer IP address.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command also will clear all MSDP statistic counters. If the MSDP peer address is not specified, the TCP connections to all MSDP peers will be cleared.

Example

This example shows how to clear the TCP connection to MSDP peer 10.1.1.1.

```
Switch#clear ip msdp peer 10.1.1.1
Switch#
```

62-19 clear ip msdp statistics

This command is used to clear the statistic counters of the specified MSDP peer.

clear ip msdp statistics [*PEER-ADDRESS***]**

Parameters

PEER-ADDRESS	(Optional) Specifies the MSDP peer IP address.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If the MSDP peer address is not specified, the statistic counters of all MSDP peers will be cleared.

Example

This example shows how to clear the statistic counter to MSDP peer 10.1.1.1.

```
Switch#clear ip msdp statistics 10.1.1.1
Switch#
```

62-20 clear ip msdp sa-cache

This command is used to clear the SA cache entries.

clear ip msdp sa-cache [*GROUP-ADDRESS***]**

Parameters

GROUP-ADDRESS	(Optional) Specifies the group address of the SA cache entry.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If the group address is not specified, all SA cache entries will be cleared.

Example

This example shows how to clear all SA cache entries.

```
Switch#clear ip msdp sa-cache
Switch#
```

62-21 show ip msdp

This command is used to display the MSDP global configuration.

show ip msdp

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the MSDP global configuration.

Example

This example shows how to display the MSDP global configuration.

```
Switch#show ip msdp

MSDP global state: Enabled
Connect retry interval: 30
SA cache expiry time: 210
SA originating filter: Configured, List: source1

Switch#
```

62-22 show ip msdp peer

This command is used to display MSDP peer information.

show ip msdp peer [*PEER-ADDRESS***]**

Parameters

PEER-ADDRESS	(Optional) Specifies the MSDP peer IP address.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MSDP peer information. If the peer IP address is specified, detailed information of the peer will be displayed. If the peer IP address is not specified, the summary information of all MSDP peers will be displayed.

Example

This example shows how to display all MSDP peers summary information.

```
Switch#show ip msdp peer

MSDP Peer Information:
Configured    Shutdown    Down    Connect    Listen    Up
3               0             2       0           0          1

Peer's Address     State     SA Count     Up/Down Time
10.1.1.1            Up         4             0DT03H04M11S
10.2.1.3            Down       0             -
10.2.1.3            Down       0             -

Switch#
```

This example shows how to display detailed information of the MSDP peer 10.1.1.1.

```
Switch#show ip msdp peer 10.1.1.1

MSDP Peer Information:
MSDP peer 10.1.1.1
Description:
Mesh Group:
Static RPF: Not configured
Information About Connection Status:
   State: Up
   Password:
   Up/Down time:  0DT03H04M41S
   Connection interface: vlan1(10.1.1.3)
   Keep-alive/Hold-time interval: 60/75
   Remote/Local port: 1024/639
   The total number of times this peer transfer into Up state: 1
Information About SA messages filter:
  Incoming filter: Not configured
  Outgoing filter: Configured, List: msdp_out
  Request filter: Configured, List: -
Minimum TTL for data-encapsulated SA message: 100
The number of SAs learned from this peer: 4
The maximum number of SAs can be learned from this peer: 20
Counters of MSDP Messages:
   Count of RPF check failure: 0
   Incoming/Outgoing control messages: 20/20
   Incoming/Outgoing SA messages: 10/10
   Incoming/Outgoing SA requests: 0/0
   Incoming/Outgoing SA responses: 0/0
   Incoming/Outgoing data packets: 0/0

Switch#
```

Display Parameters

MSDP Peer	The address of the remote MSDP peer.
Description	The MSDP peer description used to make it easier to identify.
Mesh Group	The mesh group name which this MSDP peer belongs to.
Static RPF	The static RPF configuration on this MSDP peer.
State	The state of the TCP connection with this MSDP peer. The “DISABLED” and “INACTIVE” states in RFC3618 display as “Down”, and the “ESTABLISHED” state in RFC3618 displays as “Up”.
Password	The MD5 password encryption for a TCP connection with this MSDP peer.
Up/Down Time	The system time when a MSDP peer transitions into or out of the “Up” state. It is set to zero when the MSDP router is booted.
Connection interface: vlan1(10.1.1.3)	The local IP address and IP interface used for the TCP connection to the MSDP peer.
Keep-alive/Hold-time interval	The keep-alive interval and hold-time interval. The keep-alive interval is the interval at which an MSDP peer sends keep-alive messages. The hold-time interval is the interval at which an MSDP peer will wait for keep-alive messages from other peers before declaring them as ‘down’.
Remote/Local port	The remote port and local port for the TCP connection between the MSDP peers.

The total times of this peer transfer into Up state	The total times the MSDP state transitioned into the “Up” state
Incoming filter	The SA message incoming filter configured on this MSDP peer.
Outgoing filter	The SA message outgoing filter configured on this MSDP peer.
Request filter	The SA request message filter configured on this MSDP peer.
Minimum TTL for data-encapsulated SA message	The minimum TTL of an encapsulated packet required before it may be forwarded to this peer.
The number of SAs learned from this peer.	The number of SAs learned from this peer.
The maximum number of SAs can be learned from this peer.	The maximum number of SAs can be learned from this peer.
Count of RPF check failure	The number of SA messages received from this peer that failed the Peer-RPF check.
Incoming/Outgoing control messages	The number of MSDP messages received from this peer (excluding encapsulated data packets) and transmitted to this peer.
Incoming/Outgoing SA messages	The number of MSDP SA messages received from this peer and transmitted to this peer.
Incoming/Outgoing SA requests	The number of MSDP SA request messages received from this peer and transmitted to this peer.
Incoming/Outgoing SA responses	The number of MSDP SA response messages received from this peer and transmitted to this peer.

62-23 show ip msdp sa-cache

This command is used to display SA cache information.

show ip msdp sa-cache [group *GROUP-ADDRESS***] [source** *SOURCE-ADDRESS***] [rp** *RP-ADDRESS***]**

Parameters

group *GROUP-ADDRESS*	(Optional) Specifies to display the SA cache by group address.
source *SOURCE-ADDRESS*	(Optional) Specifies to display the SA cache by source address.
rp *RP-ADDRESS*	(Optional) Specifies to display the SA cache by RP address.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display SA cache information.

Example

This example shows how to display SA cache information.

```
Switch#show ip msdp sa-cache

MSDP Source-Active Cache Information：

Group Address Source Address RP Address     Learned Peer  Up/Expire Time
230.1.1.0      192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M03S/0DT00H02M01S
230.1.1.1      192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M03S/0DT00H02M01S
230.1.1.2      192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M04S/0DT00H02M00S
230.1.1.3      192.168.120.1  192.168.122.1  10.1.1.1      0DT00H05M04S/0DT00H02M00S

Total Entries: 4

Switch#
```

62-24 show ip msdp static-rpf

This command is used to display the static RPF peer configuration.

show ip msdp static-rpf [*PEER-ADDRESS***]**

Parameters

PEER-ADDRESS	(Optional) Specifies the MSDP peer IP address.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the static RPF peer configuration.

Example

This example shows how to display the static RPF peer configuration.

```
Switch#show ip msdp static-rpf

MSDP Static RPF Peer Information：

Peer’s Address   RP List
10.1.1.1         rplist1
10.1.2.1         msdp_rp
10.1.3.2         -

Total Entries: 3

Switch#
```

62-25 show ip msdp mesh-group

This command is used to display MSDP mesh group configuration.

show ip msdp mesh-group [*PEER-ADDRESS***]**

Parameters

PEER-ADDRESS	(Optional) Specifies the MSDP peer IP address.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display MSDP mesh group configuration.

Example

This example shows how to display MSDP mesh group configuration.

```
Switch#show ip msdp mesh-group

MSDP Mesh Group Information：

Peer’s Address   Group Name
10.1.1.1         group1
10.1.2.1         group1
10.1.3.2         group1

Total Entries: 3

Switch#
```

63. Multicast VLAN Commands

63-1 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 revert to the default settings.

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 or disable 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)#
```

63-2 mvlan

This command is used to configure characteristics of the multicast VLAN feature. Use the **no** form of this command to revert to the default setting.

mvlan {forward-unmatched | ignore-vlan}

no mvlan {forward-unmatched | ignore-vlan}

Parameters

forward-unmatched	Specifies that the packet will be forwarded or dropped if the received IGMP or MLD control packet is either untagged or does not match any profile, and the

	associated default VLAN is either a multicast VLAN or is tagged with a multicast VLAN that does not match the associated profile.
ignore-vlan	Specifies the setting for tagged IGMP or MLD control packets. When this option is enabled, the Switch will ignore the VLAN of the receiving IGMP or MLD control packet, and try to find a matching profile.

Default

By default, forward-unmatched is disabled, and the packet is dropped.

By default, ignore VLAN is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If an untagged IGMP/MLD report/leave/done packet is received by a port, it will be matched against the multicast VLAN group profile that the port belongs to. If it matches, it will be classified as belonging to the corresponding multicast VLAN and handled by the 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 forwarded to VLAN member ports depending on the setting of the **forward-unmatched** parameter. If the **no mvlan forward-unmatched** command is configured, the packet is dropped. If the **mvlan forward-unmatched** command is configured, the packet is forwarded.

If there are no matches against all multicast VLANs and the packet's VLAN is not configured as the multicast VLAN, the IGMP/MLD packet will not be handled by the multicast VLAN.

If the IGMP/MLD report/leave/done packet received by the receiver port is tagged, the handling is different based on setting of the **ignore-vlan** parameters.

If the packet VLAN is a multicast VLAN and the packet matches the group profile of the VLAN, the packet will be handled by the subsequent group learning process. If there is no match, the packet will be handled based on the setting of the **forward-unmatched** parameter. If the packet VLAN is not a multicast VLAN, the packet will not be handled by the multicast VLAN.

If the packet VLAN is IGMP/MLD snooping enabled, the packet will be processed by IGMP/MLD snooping. If the packet VLAN is IGMP/MLD snooping disabled, the VLAN is ignored and the multicast VLAN group profile associated with the port is used. If there is a match, the packet will be handled by the subsequent group learning process with the matched multicast VLAN. If there is no match but the packet VLAN is a multicast VLAN, the packet will be handled based on the setting of the **forward-unmatched** parameter. If the packet VLAN is not a multicast VLAN, 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)#
```

63-3 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-ID	Specifies the multicast VLAN. 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)#
```

63-4 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, the packets will be forwarded in the untagged form.
INTERFACE-ID	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

No 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 port. If IGMP/MLD report packets come from a source port, the 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 1 to 4 as tagged receiver ports in multicast VLAN 100.

```
Switch#configure terminal
Switch(config)#mvlan vlan 100
Switch(config-mvlan)#member receiver tagged eth1/0/1-4
Switch(config-mvlan)#
```

63-5 name

This command is used to specify the name of a multicast VLAN. Use the **no** form of this command to revert to the default setting.

name *VLAN-NAME*

no name

Parameters

VLAN-NAME	Specifies the VLAN name, with a maximum of 32 characters.

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 vlan 100
Switch(config-mvlan)#name ip-tv
Switch(config-mvlan)#
```

63-6 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 uses 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 vlan 100
Switch(config-mvlan)#replace-priority ipv4 4
Switch(config-mvlan)#
```

63-7 replace-source-ip

This command is used to replace the source IP address in the reporting IGMP/MLD packet sent to uplink ports. Use the **no** form of this command to cancel the replacement.

replace-source-ip {ipv4 *IPV4-ADDRESS* **| ipv6** *IPV6-ADDRESS***} from { source | receiver | both}**

no replace-source-ip {ipv4 | ipv6}

Parameters

ipv4 *IPV4-ADDRESS*	Specifies the source IP address to be substituted for the source IP address in the reporting IGMP control packet to uplink ports.
ipv6 *IPV6-ADDRESS*	Specifies the source IP address to be substituted for the source IP address in the reporting MLD control packet to uplink ports.
source	Specifies to replace the source IP address of the IGMP or MLD report/leave/done packet received on any multicast VLAN source port with the specified IPv4 or IPv6 address.
receiver	Specifies to replace the source IP address of the IGMP or MLD report/leave/done packet received on any multicast VLAN receiver port with the specified IPv4 or IPv6 address.
both	Specifies to replace the source IP address of the IGMP or MLD report/leave/done packet received on any port in the multicast VLAN with the specified IPv4 or IPv6 address.

Default

None.

Command Mode

Multicast VLAN Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to report the join information to the source port. The purpose is to avoid the control packets being 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 vlan 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)#
```

63-8 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. Multicast VLANs will check if the group address in the IGMP/MLD packet matches the range of addresses defined in this profile.

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)#
```

63-9 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 with multicast VLANs. If a port is a member of more than one multicast VLAN, the **group-profile** bound to the multicast VLAN will decide which multicast VLAN can learn the group.

If a port is member of a single multicast VLAN and an access group is configured for the multicast VLAN, only those groups permitted by the access group are learned with the multicast VLAN. If there is no access group configured, all multicast groups 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 vlan 100
Switch(config-mvlan)#access-group mv_profile1
Switch(config-mvlan)#
```

63-10 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 in the range.
IPV4-ADDRESS-END	Specifies the IPv4 multicast end address in the range.
IPV6-ADDRESS-START	Specifies the IPv6 multicast start address in the range.
IPV6-ADDRESS-END	Specifies the IPv6 multicast end address in 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 in 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)#
```

63-11 show mvlan group-profile

This command is used to display the multicast group profile configuration.

show mvlan group-profile [*PROFILE-NAME***]**

Parameters

PROFILE-NAME	(Optional) Specifies the profile name.

Default

None.

Command Mode

User/Privileged EXEC 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 Address
-----------------               ---------------------
mv_profile1                     225.0.0.0 - 225.0.0.5

Total Entries: 1

Switch#
```

63-12 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	(Optional) Specifies the VLAN ID.

Default

None.

Command Mode

User/Privileged EXEC 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

Total Entries: 1

Switch#
```

63-13 show mvlan

This command is used to display multicast VLAN configurations.

show mvlan [*VLAN-ID***]**

Parameters

VLAN-ID	(Optional) Specifies the VLAN ID.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no optional parameter is specified, all configuration and multicast VLAN information will be displayed.

Example

This example shows how to display all multicast VLAN configuration and information on the Switch.

```
Switch#show mvlan

IPv4 Multicast VLAN State     : Enabled
IPv6 Multicast VLAN State     : Disabled
Forward Unmatched             : Disabled
Ignore VLAN                   : Disabled

MVLAN 100
  Name                  : ip-tv
  Untagged Receiver     :
  Tagged Receiver       : 1/0/1-1/0/4
  Untagged Source       :
  Tagged Source         :
  Replace Source IP     : 1.10.10.10 (from receiver)/FE80:3000::3 (from source)
  Replace Priority      : 4 (IPv4)/Not replace (IPv6)


Total Entries: 1

Switch#
```

Display Parameters

IPv4 Multicast VLAN State	The state of the multicast VLAN process for IPv4 packet.
IPv6 Multicast VLAN State	The state of the multicast VLAN process for IPv6 packets.
Forward Unmatched	The forwarding mode for Multicast VLAN unmatched packets. **Enabled** means to forward unmatched packets, and **Disabled** means to drop unmatched packets.

Ignore VLAN	Ignore the VLAN tag of IGMP control packets and automatically assign IGMP control packets to the correct multicast VLAN to process.
Untagged/Tagged Receiver/Source	The receiver or source ports configured in multicast VLAN, and the VLAN tagged or untagged attribute for multicast packets forwarded to them.
Replace Source IP	The source IP address that will be replaced in the IGMP/MLD control packets before being forwarded in the multicast VLAN.

64. Multiple Spanning Tree Protocol (MSTP) Commands

64-1 instance

This command is used to map VLANs to an MST instance. Use the **no instance** *INSTANCE-ID* command to remove the specified MST instance. Use the **no instance** *INSTANCE-ID* **vlans** *VLAND-ID* **[, | -]** command to return the VLANs to the default instance (CIST).

instance *INSTANCE-ID* **vlans** *VLAN-ID* **[, | -]**

no instance *INSTANCE-ID* **[vlans** *VLAN-ID* **[, | -]]**

Parameters

INSTANCE-ID	Specifies the MSTP instance identifier that is mapped with the specified VLANs. The value is from 1 to 64.
VLAN-ID	Specifies the VLAN ID to be configured.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, all VLANs are mapped with the CIST (instance 0).

Command Mode

MST Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to map VLANs to an MST instance. When mapping VLANs to a MST instance, the instance will be created automatically if the instance does not exist.

Example

This example shows how to map VLANs to an MST instance.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#instance 2 vlans 1-100
Switch(config-mst)#
```

64-2 name

This command is used to configure the name of an MST region. Use the **no** form of this command to revert to the default setting.

name *NAME*

no name

Parameters

NAME	Specifies the name for the MST region. The maximum length is 32 characters.

Default

By default, the name is the bridge MAC address.

Command Mode

MST Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the name of an MST region. When more than one switch with the same VLAN mapping and configuration version number, but with different region names, they are considered to be in different MST regions.

Example

This example shows how to configure the name of the MST region as “MSTP”.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#name MSTP
Switch(config-mst)#
```

64-3 revision

This command is used to configure the revision number for the MST configuration. Use the **no** form of this command to revert to the default setting.

revision *REVISION*

no revision

Parameters

REVISION	Specifies the different revision level when the name is the same. The value is from 0 to 65535.

Default

By default, the value is 0.

Command Mode

MST Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the revision number for the MST configuration. When more than one switch with the same configuration but different revision numbers, they are considered to be in different MST regions.

Example

This example shows how to configure the revision number for the MST configuration to “2”.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#revision 2
Switch(config-mst)#
```

64-4 show spanning-tree mst

This command is used to display the information of Multiple Spanning Tree (MST) and instances.

show spanning-tree mst [configuration [digest]]

show spanning-tree mst [instance *INSTANCE-ID* **[, | -]] [interface** *INTERFACE-ID* **[, | -]] [detail]**

Parameters

configuration	(Optional) Specifies the MST configuration of the equipment.
digest	(Optional) Specifies to display the MD5 digest included in the current MST configuration identifier (MSTCI).
instance *INTANCE-ID*	(Optional) Specifies the instance number to be displayed.
,	(Optional) Specifies a series of instances or separates a range of instances from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of instances. No space is allowed before or after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
detail	(Optional) Specifies to display detailed MST information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display MST information.

Example

This example shows how to display spanning tree configuration information on port 1.

```
Switch#show spanning-tree mst configuration

 Name      : F0:7D:68:34:00:10
 Revision  : 0,Instances configured: 1
 Instance    Vlans
 -------     ------------------------------------------------------------
      0      1-4094

Switch#
```

64-5 spanning-tree mst

This command is used to configure the path cost and port priority for the MST instance. Use the **no** form of this command to revert to the default settings.

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. The value is from 0 to 64. The value 0 represents the default instance, CIST.
cost *COST*	Specifies the path cost of the instance. The value is from 1 to 200000000.
port-priority *PRIORITY*	Specifies the port priority of the instance. The value is from 0 to 240 in increments of 16.

Default

The cost is defined based on the port speed. The faster the speed is, the smaller cost value it is. MST always uses long path cost.

The port priority is 128.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for the physical ports.

Example

This example shows how to configure the interface path cost.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree mst 0 cost 17031970
Switch(config-if)#
```

This example shows how to configure the port priority.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree mst 0 port-priority 64
Switch(config-if)#
```

64-6 spanning-tree mst configuration

This command is used to enter the MST configuration mode and configure the MSTP region. Use the **no** form of this command to revert all settings in the MST configuration mode to the default settings.

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

Use this command to enter the MST configuration mode.

Example

This example shows how to enter the MST configuration mode.

```
Switch#configure terminal
Switch(config)#spanning-tree mst configuration
Switch(config-mst)#
```

64-7 spanning-tree mst max-hops

This command is used to configure the MSTP maximum hop count. Use the **no** form of this command to revert to the default setting.

spanning-tree mst max-hops *HOP-COUNT*

no spanning-tree mst max-hops

Parameters

HOP-COUNT	Specifies the MSTP maximum hop count. The value is from 1 to 40.

Default

By default the MSTP maximum hop count is 20.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the MSTP maximum hop count.

Example

This example shows how to configure the MSTP maximum hop count.

```
Switch#configure terminal
Switch(config)#spanning-tree mst max-hops 19
Switch(config)#
```

64-8 spanning-tree mst hello-time

This command is used to configure the hello time used in MSTP version for each port. Use the **no** form of this command to revert to the default setting.

spanning-tree mst hello-time *SECONDS*

no spanning-tree mst hello-time

Parameters

SECONDS	Specifies the interval of sending one BPDU at the designated port. The range is from 1 to 2 seconds.

Default

By default, the hello-time is 2 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the hello time used in MSTP version for each port. This only takes effects in the MSTP mode.

Example

This example shows how to configure the hello time used in MSTP version on port 1.

```
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree mst hello-time 1
Switch(config-if)#
```

64-9 spanning-tree priority

This command is used to configure the bridge priority value for the selected MSTP instance. Use the **no** form of this command to revert to the default setting.

spanning-tree mst *INSTANCE-ID* **priority** *PRIORITY*

no spanning-tree mst *INSTANCE-ID* **priority**

Parameters

INSTANCE-ID	Specifies the MSTP instance identifier. Instance 0 represents the default instance, CIST.
PRIORITY	Specifies 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 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)#
```

65. Neighbor Discovery (ND) Inspection Commands

65-1 ipv6 nd inspection policy

This command is used to create an ND inspection policy. This command will enter the ND Inspection Policy Configuration Mode. Use the **no** form of this command to remove the ND inspection policy.

ipv6 nd inspection policy *POLICY-NAME*

no ipv6 nd inspection policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the ND inspection policy name.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to create an ND inspection policy. This command will enter the ND Inspection Policy Configuration Mode. ND inspection is mainly for inspection of Neighbor Solicitation (NS) and Neighbor Advertisement (NA) messages.

Example

This example shows how to create an ND policy name called “policy1”.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#
```

65-2 validate source-mac

This command is used to check the source MAC address against the link-layer address for ND messages. Use the **no** form of this command to disable the check.

validate source-mac

no validate source-mac

Parameters

None.

Default

By default, this option is disabled.

Command Mode

ND Inspection Policy Configuration Mode.

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)#
```

65-3 device-role

This command is used to specify the role of the attached device. Use the **no** form of this command to revert to the default setting.

device-role {host | router}

no device-role

Parameters

host	Specifies to set the role of the device to host.
router	Specifies to set the role of the device to router.

Default

By default, the device's role is host.

Command Mode

ND Inspection Policy Configuration Mode.

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 an 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)#
```

65-4 mode

This command is used to specify the mode of ND inspection. Use the **no** form of this command to revert to the default setting.

mode {precise | fuzzy}

no mode

Parameters

precise	Specifies to use the precise mode.
fuzzy	Specifies to use the fuzzy mode.

Default

By default, the mode is **precise**.

Command Mode

ND Inspection Policy Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command is used to specify the mode of ND inspection. When the mode is configured to **precise**, ND inspection checks if target address is the same as source address in DANA/NA packets. When the mode is configured to **fuzzy**, ND inspection checks if both target and source addresses exist in the binding table.

Example

This example shows how to create an ND policy named “policy1” and configures the mode to **fuzzy**.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#mode fuzzy
Switch(config-nd-inspection)#
```

65-5 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 only available for physical port and port-channel interface 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 port 3.

```
Switch#configure terminal
Switch(config)#ipv6 nd inspection policy policy1
Switch(config-nd-inspection)#device-role host
Switch(config-nd-inspection)#validate source-mac
Switch(config-nd-inspection)#exit
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 nd inspection attach-policy policy1
Switch(config-if)#
```

65-6 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/Privileged EXEC 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#
```

66. Network Access Authentication Commands

66-1 authentication guest-vlan

This command is used to configure the guest VLAN setting. Use the **no** form of this command to remove the guest VLAN.

authentication guest-vlan *VLAN-ID*

no authentication guest-vlan

Parameters

VLAN-ID	Specifies the authentication guest VLAN.

Default

None.

Command Mode

Interface Configuration Mode.

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, 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)#
```

66-2 authentication host-mode

This command is used to specify the authentication mode. Use the **no** form of this command to revert to the default setting.

authentication host-mode {multi-host | multi-auth [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.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, **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 one of the hosts is authenticated, all other hosts are allowed to access the port. According to 802.1X authentication, if the re-authentication fails or the authenticated user logs off, the port will be blocked for a quiet period. The port restores the processing of EAPOL packets after the quiet period.

If the port is operated in the **multi-auth** mode, each host needs to be authenticated individually to access the port. A host is represented by its MAC address. Only the authorized host is allowed to access.

Example

This example shows how to specify the port 1 to operate in the multi-host mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication host-mode multi-host
Switch(config-if)#
```

66-3 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. Use the **authentication timer reauthentication** command to configure the re-authentication timer.

Example

This example shows how to enable periodic re-authentication on port 1.

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

66-4 authentication timer inactivity

This command is used to configure the timer after which an inactive session is terminated. Use the **no** form of this 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 the **authentication timer reauthentication** command.

Example

This example shows how to configure the inactivity timer to 240 for port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer inactivity 240
Switch(config-if)#
```

66-5 authentication timer reauthentication

This command is used to configure the timer to re-authenticate a session. Use the **no** form of this command to revert 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. Use the **authentication periodic** command to determine whether re-authentication will occur.

Example

This example shows how to configure the re-authentication timer value to 200 for port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer reauthentication 200
Switch(config-if)#
```

66-6 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 this command to revert to the default setting.

authentication timer restart *SECONDS*

no authentication timer restart

Parameters

SECONDS	Specifies the authentication restart timer value. The range is from 1 to 65535.

Default

By default, this value is 60 seconds.

Command Mode

Interface Configuration Mode.

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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication timer restart 20
Switch(config-if)#
```

66-7 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 *PASSWORD*	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*	(Optional) Specifies the VLAN to be assigned.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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)#
```

66-8 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 port 1.

```
Switch#clear authentication sessions interface eth1/0/1
Switch#
```

66-9 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 revert 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)#
```

66-10 authentication compauth mode

This command is used to specify the compound authentication mode. Use the **no** form of this command to revert to the default setting.

authentication compauth mode {any | mac-wac}

no authentication compauth mode

Parameters

any	Specifies to pass if any of the authentication methods (802.1X, MAC-based Access Control and WAC) passes. If this parameter is used but MAC-based Access Control is disabled and 802.1X is enabled, 802.1X authentication will still be required.
mac-wac	Specifies to verify MAC-based Access Control first. If the client passed MAC authentication, WAC will be verified. Both authentication methods need to be passed to have a successful authentication. If this parameter is used, authorized access will be given after two methods of authentication have passed. If any of the authentication methods have failed, access will be rejected. If the related authentication method's global or port state is not enabled, access will also be rejected. After authenticated, the authorized information will be taken from the WAC module.

Default

By default, the option is **any**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the authentication methods on physical ports.

Example

This example shows how to configure port 1 to operate in the mac-wac mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#authentication compauth mode mac-wac
Switch(config-if)#
```

66-11 authentication max users

This command is used to configure the maximum authenticated users for the entire system or for a port. Use the **no** form of this command to revert to the default 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

By default, there is no limit.

Command Mode

Global Configuration Mode.

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the command is configured in the Global Configuration Mode, the maximum user number limits the user number of the entire system.

When 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)#
```

66-12 authentication mac-move deny

This command is used to deny MAC move on the Switch. Use the **no** form of this command to revert to the default setting.

authentication mac-move deny

no authentication mac-move deny

Parameters

None.

Default

By default, this option is permitted.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command controls 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, 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, 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, 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, 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)#
```

66-13 authorization disable

This command is used to disable the acceptance of the authorized configuration. Use the **no** form of this command 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)#
```

66-14 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	(Optional) Specifies to display all MAC sessions.
wac	(Optional) Specifies to display all WAC sessions.
dot1x	(Optional) Specifies to display all dot1x sessions.
interface *INTERFACE-ID*	(Optional) Specifies a port to display.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
mac-address *MAC-ADDRESS*	(Optional) Specifies to display a specific user.

Default

None.

Command Mode

User/Privileged EXEC 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 port 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.
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, 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.

67. Network Load Balancing (NLB) Commands



NOTE: When the NLB feature is enabled, link aggregation member ports cannot exist on different switches in the physical switch stack.

67-1 nlb unicast-fdb

This command is used to add a unicast MAC entry to the NLB unicast address table. Use the **no** form of this 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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

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 the NLB unicast address 00-F3-22-0A-12-F4 to the MAC address table. The candidate forwarding interfaces are on ports 1 to 5.

```
Switch#configure terminal
Switch(config)#nlb unicast-fdb 00-F3-22-0A-12-F4 interface eth1/0/1-5
Switch(config)#
```

67-2 nlb multicast-fdb

This command is used to add an entry to the NLB multicast address table. Use the **no** form of this 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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Global Configuration Mode.

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 the multicast address 01-F3-22-0A-12-F4 received on VLAN 1 candidate forwarding ports 1 to 5 to the NLB multicast address table.

```
Switch#configure terminal
Switch(config)#nlb multicast-fdb 01-F3-22-0A-12-F4 vlan 1 interface eth1/0/1-5
Switch(config)#
```

67-3 show nlb fdb

This command is used to display NLB configured entries.

show nlb fdb

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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
 ----------------- ---------- -------------------------------------------------
 00-11-22-33-44-55 ----       eth 1/0/20

Total Entries :1

Switch#
```

68. Network Protocol Port Protection Commands

68-1 network-protocol-port protect

This command is used to enable the network protocol port protection function. Use the **no** form of this command to disable this function.

network-protocol-port protect {tcp | udp}

no network-protocol-port protect {tcp | udp}

Parameters

tcp	Specifies to protect the TCP port.
udp	Specifies to protect the UDP port.

Default

By default, this function is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the network protocol port protection function.

Example

This example shows how to enable TCP port protection.

```
Switch#configure terminal
Switch(config)#network-protocol-port protect tcp
Switch(config)#
```

68-2 show network-protocol-port protect

This command is used to display the information of the network protocol port protection.

show network-protocol-port protect

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the information of the network protocol port protection.

Example

This example shows how to display the information of the network protocol port protection.

```
Switch#show network-protocol-port protect

     TCP Port protect state: Enabled
     UDP Port protect state: Enabled

Switch#
```

69. Network Time Protocol (NTP) Commands

69-1 ntp access-group

This command is used to control the NTP services on the Switch. Use the **no** form of this command to remove the access control to the NTP services.

ntp access-group {default | *IP-ADDRESS* **[***IP-MASK***] |** *IPV6-ADDRESS* **|** *IPV6-ADDRESS /PREFIX-LENGTH***} [ignore] [nomodify] [noquery] [nopeer] [noserve] [notrust] [version]**

no ntp access-group {default | *IP-ADDRESS* **[***IP-MASK***] |** *IPV6-ADDRESS* **|** *IPV6-ADDRESS* /PREFIX-LENGTH**}**

Parameters

default	Specifies to use the default IPv4 (0.0.0.0/0.0.0.0) or IPv6 (::/::) address. The default IP address is always included with the lowest priority in the list.
IP-ADDRESS	Specifies a host or network IP address.
IP-MASK	(Optional) Specifies the mask of the IP address.
IPV6-ADDRESS	Specifies a host or network IPv6 address.
IPV6-ADDRESS /PREFIX-LENGTH	(Optional) Specifies an IPv6 network.
ignore	(Optional) Specifies to deny all packets, including NTP control queries.
nomodify	(Optional) Specifies to deny the NTP control queries that attempt to modify the state of the server.
noquery	(Optional) Specifies to deny all NTP control queries.
nopeer	(Optional) Specifies to deny packets that might mobilize an association unless authenticated. The packets include broadcast, symmetric-active and manycast server packets when a configured association does not exist. Note that this flag does not apply to packets that do not attempt to mobilize an association.
noserve	(Optional) Specifies to deny all packets except NTP control queries.
notrust	(Optional) Specifies to deny packets that are not cryptographically authenticated. If the **ntp authenticate** command is enabled, authentication is required for all packets that might mobilize an association. If the **ntp authenticate** command is disabled, but the notrust flag is not present, an association can be mobilized no matter it is authenticated or not. If auth is disabled, but the notrust flag is present, authentication is required only for the specified address/mask range.
version	(Optional) Specifies to deny packets that mismatch the current NTP version

Default

By default, **noquery** and **nomodify** is set on the default entry to prevent the Denial of Service vulnerability in the NTP service identified in “NTP.Monlist.Command.DoS”.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The NTP implements a general purpose Access Control List (ACL) containing address/match entries sorted first by increasing address values and then by increasing mask values. A match occurs when the bitwise AND of the mask and the packet source address is equal to the bitwise AND of the mask and address in the list. The list is searched in order with the last match found defining the restriction flags associated with the entry.

Example

This example shows how to deny new associations by default except for 192.43.244.18, 128.175.0.0/16, and 128.4.1.0/24 (need authentication).

```
Switch#configure terminal
Switch(config)#ntp access-group default nopeer
Switch(config)#ntp access-group 128.175.0.0 255.255.0.0
Switch(config)#ntp access-group 128.4.1.0 255.255.255.0 notrust
Switch(config)#ntp access-group 192.43.244.18
Switch(config)#
```

69-2 ntp authenticate

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

ntp authenticate

no ntp authenticate

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When this feature is enabled, networking nodes will not synchronize with the Switch unless it carries one of the authentication keys specified in the **ntp trusted-key** command.

Example

This example shows how to enable NTP authentication.

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

69-3 ntp authentication-key

This command is used to define an authentication key for NTP. Use the **no** form of this command to remove the key.

ntp authentication-key *KEY-ID* **md5** *VALUE*

no ntp authentication-key *KEY-ID*

Parameters

KEY-ID	Specifies the NTP key ID. The value is from 1 to 255.
md5	Specifies the authentication key type to MD5.
VALUE	Specifies the key string. This string must be 32 characters long.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to define an authentication key for NTP. Use the **no** form of this command to remove the key.

Example

This example shows how to define an authentication key with the key ID “45” and key string “NTPKey”.

```
Switch#configure terminal
Switch(config)#ntp authentication-key 45 md5 NTPKey
Switch(config)#
```

69-4 ntp control-key

This command is used to define the key ID for the NTP control messages. Use the **no** form of this command to remove the key.

ntp control-key *KEY-ID*

no ntp control-key

Parameters

KEY-ID	Specifies the NTP key ID. The value is from 1 to 255.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to define the key ID for the NTP control messages.

Example

This example shows how to define a key ID for the NTP control messages.

```
Switch#configure terminal
Switch(config)#ntp control-key 45
Switch(config)#
```

69-5 ntp disable

This command is used to prevent an interface from receiving NTP packets. Use the **no** form of this command to receive NTP packets on an interface.

ntp disable

no ntp disable

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 configure whether to receive NTP packets on an interface an interface.

Example

This example shows how to prevent VLAN 1 interface from receiving NTP packets.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ntp disable
Switch(config-if)#
```

69-6 ntp master

This command is used to configure the NTP master stratum value. Use the **no** form of this command to disable this feature.

ntp master *STRATUM*

no ntp master

Parameters

STRATUM	Specifies the NTP stratum number between 1 and 15.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the command to configure the NTP master stratum value.

Example

This example shows how to configure the NTP master stratum value to 10.

```
Switch#configure terminal
Switch(config)#ntp master 10
Switch(config)#
```

69-7 ntp max-associations

This command is used to configure the maximum number of NTP peers and clients on the Switch. Use the **no** form of this command to revert to the default setting.

ntp max-associations *NUMBER*

no ntp max-associations

Parameters

NUMBER	Specifies the number of NTP associations. This value must be between 1 and 64.

Default

By default, the value is 32.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the maximum number of NTP peers and clients on the Switch.

Example

This example shows how to configure the maximum number of NTP associations to 20.

```
Switch#configure terminal
Switch(config)#ntp max-associations 20
Switch(config)#
```

69-8 ntp peer

This command is used to configure the NTP peer settings. Use the **no** form of this command to disable this feature.

ntp peer {*IP-ADDRESS* | *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**

no ntp peer {*IP-ADDRESS* | *IPv6-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the peer.
IPv6-ADDRESS	Specifies the IPv6 address of the peer.
version	(Optional) Specifies the NTP version number.
NUMBER	(Optional) Specifies to enter the NTP version number from 1 to 4. The default version number is 4.
key	(Optional) Specifies the authentication key.
KEY-ID	(Optional) Specifies to enter the authentication key ID from 1 to 255.
prefer	(Optional) Specifies to be the preferred peer for synchronization.
min-poll	(Optional) Specifies the minimum poll interval for NTP messages. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds (2^6=64).
INTERVAL	(Optional) Specifies to enter the minimum poll interval value. The default value is 6.
max-poll	(Optional) Specifies the maximum poll interval for NTP messages. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds (2^6=64).
INTERVAL	(Optional) Specifies to enter the maximum poll interval value. The default value is 10.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The Switch's software clock can synchronize the NTP settings with a peer.

Example

This example shows how to configure the IP address of the NTP peer to 192.168.22.33 using NTP version 3.

```
Switch#configure terminal
Switch(config)#ntp peer 192.168.22.33 version 3
Switch(config)#
```

69-9 ntp request-key

This command is used to define the key ID for NTP mode 7 packets, used by the *ntpdc* utility program. Use the **no** form of this command to remove the key.

ntp request-key *KEY-ID*

no ntp request-key

Parameters

KEY-ID	Specifies the NTP key ID. The value is from 1 to 255.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The ntpdc utility program uses a proprietary protocol specific to the implementation of NTP.

Example

This example shows how to define the NTP request key.

```
Switch#configure terminal
Switch(config)#ntp request-key 45
Switch(config)#
```

69-10 ntp server

This command is used to enable the Switch to synchronize the time with an NTP server. Use the **no** form of this command to disable this feature.

ntp server {*IP-ADDRESS* **|** *IPv6-ADDRESS***} [version** *NUMBER***] [key** *KEY-ID***] [prefer] [min-poll** *INTERVAL***] [max-poll** *INTERVAL***]**

no ntp server {*IP-ADDRESS* **|** *IPv6-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the NTP server.
IPv6-ADDRESS	Specifies the IPv6 address of the NTP server.
version	(Optional) Specifies the NTP version number.
NUMBER	(Optional) Specifies to enter the NTP version number from 1 to 4. The default version number is 4.
key	(Optional) Specifies the authentication key.
KEY-ID	(Optional) Specifies the authentication key ID from 1 to 255.
prefer	(Optional) Specifies to be the preferred peer for synchronization.
min-poll	(Optional) Specifies the minimum poll interval for NTP messages. This value is calculated as 2 to the power of the minimum poll interval value specified. For example, if the value specified here is 6, the minimum poll interval that will be used is 64 seconds (2^6=64).
INTERVAL	(Optional) Specifies to enter the minimum poll interval value. The default value is 6.
max-poll	(Optional) Specifies the maximum poll interval for NTP messages. This value is calculated as 2 to the power of the maximum poll interval value specified. For example, if the value specified here is 6, the maximum poll interval that will be used is 64 seconds (2^6=64).
INTERVAL	(Optional) Specifies to enter the maximum poll interval value. The default value is 10.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the Switch to synchronize the time with an NTP server.

Example

This example shows how to configure the IP address of the NTP server to 192.168.10.33 using NTP version 2.

```
Switch#configure terminal
Switch(config)#ntp server 192.168.10.33 version 2
Switch(config)#
```

69-11 ntp trusted-key

This command is used to specify the trusted key for a peer NTP system to authenticate. Use the **no** form of this command to disable this feature.

ntp trusted-key *KEY-ID*

no ntp trusted-key *KEY-ID*

Parameters

KEY-ID	Specifies the NTP key ID. The value is from 1 to 255.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the trusted key for a peer NTP system to authenticate. Use the **no** form of this command to disable this feature.

Example

This example shows how to configure the NTP trusted key.

```
Switch#configure terminal
Switch(config)#ntp trusted-key 45
Switch(config)#
```

69-12 ntp update-calendar

This command is used to periodically update the hardware clock from an NTP source. Use the **no** form of this command to disable this feature.

ntp update-calendar

no ntp update-calendar

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 periodically update the hardware clock from an NTP source. Use the **no** form of this command to disable this feature.

Example

This example shows how to periodically update the hardware clock from an NTP source.

```
Switch#configure terminal
Switch(config)#ntp update-calendar
Switch(config)#
```

69-13 service ntp

This command is used to enable NTP. Use the **no** form of this command to disable this feature.

service ntp

no service ntp

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 configure the NTP global state.

Example

This example shows how to enable NTP.

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

69-14 show ntp associations

This command is used to display the status of NTP associations.

show ntp associations [detail]

Parameters

detail	(Optional) Specifies to display detail information about each NTP association.

Default

Not applicable.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the status of NTP associations.

Example

This example shows how to display the NTP associations.

```
Switch#show ntp associations

     Remote           Local      St Poll Reach  Delay   Offset    Disp
==============================================================================
=192.168.10.33   0.0.0.0        16  128    0 0.00000  0.000000 3.99217
+192.168.22.33   0.0.0.0        16  128    0 0.00000  0.000000 3.99217
+ Symmetric active, - Symmetric passive, = Client, * System Peer

Switch#
```

Display Parameters

Leading Characters	The first characters in a display line can be one of the following characters: **+** - Symmetric active mode. **-** - Symmetric passive mode. **=** - Client mode. **^** - Broadcast mode. **~** - Broadcast client.

	* - System Peer.
Remote	The IP address of the peer.
Local	The IP address of the local interface.
St	Stratum of the peer.
Poll	Polling interval in seconds.
Reach	Peer reaching ability.
Delay	Round-trip delay to peer in milliseconds.
Offset	Relative time of peer clock to local clock in milliseconds.
Disp	Dispersion.

This example shows how to display the NTP associations in detail.

```
Switch#show ntp associations detail

Remote 192.168.10.33, Local 0.0.0.0
Our mode client, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 2, Association 8356
Reach 000, Unreach 17, Flash 0x1400, Timer 840s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Originate Timestamp: 00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Receive Timestamp:   00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Transmit Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
Filter Delay:  0.00000  0.00000  0.00000  0.00000
               0.00000  0.00000  0.00000  0.00000
Filter Offset: 0.000000 0.000000 0.000000 0.000000
               0.000000 0.000000 0.000000 0.000000
Filter Order:  0        1        2        3
               4        5        6        7
Offset 0.000000, Delay 0.00000, Error Bound 3.99217, Filter Error 0.00000

Remote 192.168.22.33, Local 0.0.0.0
Our mode sym_active, Peer mode unspec, Stratum 16, Precision -7
Leap 11, RefID [INIT], RootDistance 0.00000, RootDispersion 0.00000
PPoll 10, HPoll 10, KeyID 0, Version 3, Association 8355
Reach 000, Unreach 17, Flash 0x1400, Timer 798s, flags  Config
Reference Timestamp:  00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Display Parameters

Remote	The IP address of the peer.
Local	The IP address of the Switch.
Our mode	Our mode relative to the peer. This field can display the following modes: **active**, **passive**, **client**, **server**, **bdcast**, and **bdcastclient**.
Peer mode	The peer's mode relative to us.
Stratum	Stratum of the peer.
Precision	Precision value.
Leap	Leap indicator. The value is from 0 to 3.
RefID	The IP address of the machine peer is synchronized to.

RootDistance	The total roundtrip delay to the primary reference clock.
RootDispersion	The total root dispersion to the primary reference clock.
PPoll	The peer poll exponent.
HPoll	The host poll exponent.
KeyID	Authentication key ID.
Version	The NTP version that the peer is using.
Association	The Association ID.
Reach	Peer reaching ability.
Unreach	Unreached counter.
Flash	Flash status word for diagnosing problems.
Timer	The peer timer in seconds.
Flags	The peer flags.
Reference Timestamp	The time that the system clock was last set or corrected.
Originate Timestamp	The time that the request departed for the server at the client.
Receive Timestamp	The time that the request arrived from the client at the server.
Transmit Timestamp	The time that replied to the client at the server.
Filter Delay	Round-trip delay of each sample in milliseconds.
Filter Offset	Clock offset of each sample in milliseconds.
Filter Order	Filter order of each sample.
Offset	Offset of the peer clock relative to our clock.
Delay	Round-trip delay to the peer.
Error Bound	Peer dispersion.
Filter Error	Approximate error of each sample.
St	Stratum of the peer.
Poll	Polling interval in seconds.
Reach	Peer reaching ability.
Delay	Round-trip delay to peer in milliseconds.
Offset	Relative time of peer clock to local clock in milliseconds.
Disp	Dispersion.

69-15 show ntp status

This command is used to display the NTP status.

show ntp status

Parameters

None.

Default

Not applicable.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the NTP status.

Example

This example shows how to display NTP status.

```
Switch#show ntp status

Leap Indicator:       Unsynchronized
Stratum:              16
Precision:            -8
Root Distance:        0.00000 s
Root Dispersion:      0.10680 s
Reference ID:         [INIT]
Reference Time:       00000000.00000000  Thu, Feb  7 2036  6:28:16.00000
System Flags:         Auth Monitor NTP Kernel Stats
Jitter:               0.000000 s
Stability:            0.000 ppm
Auth Delay:           0.000000 s

Switch#
```

Display Parameters

Remote	The IP address of the peer.
Local	The IP address of the Switch.
Our mode	Our mode relative to the peer. This field can display the following modes: **active**, **passive**, **client**, **server**, **bdcast**, and **bdcastclient**.
Peer mode	The peer's mode relative to us.
Leap Indicator	**Synchronized** - The Switch is synchronized to an NTP peer. **Unsynchronized** - The Switch is not synchronized to any NTP peer.
Stratum	Stratum of the Switch.
Precision	Precision value.
Root Distance	The total roundtrip delay to the primary reference clock.
Root Dispersion	The dispersion of the root path.
Reference ID	The IP address of the peer that the Switch is synchronized to.
Reference Time	Reference time stamp.
System Flags	**Auth** – Requires authentication to configure. **Monitor** - Enables the monitor. **NTP** - The clock discipline is enabled. **Kernel** - The kernel support is enabled. **Stats** – System status control.
Jitter	System jitter.

Stability	Frequency stability (wander) (s/s).
Auth Delay	Authentication Delay.

70. Open Shortest Path First Version 2 (OSPFv2) Commands

70-1 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** form of this 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)#
```

70-2 area nssa

This command is used to assign an area as an NSSA area. Use the **no** form of this 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.

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.

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)#
```

70-3 area range

This command is used to summarize OSPF routes at an area border router. Use the **no** form of this command to remove the defined summarization of routes.

area *AREA-ID* **range** *NETWORK-PREFIX NETWORK-MASK* **[advertise | no-advertise]**

no area *AREA-ID* **range** *NETWORK-PREFIX NETWORK-MASK*

Parameters

AREA-ID	Specifies the area from which the routes will be summarized.
NETWORK-PREFIX	Specifies the network prefix of the summary route.
NETWORK-MASK	Specifies the network mask 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.

By default, **advertise** is specified.

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)#
```

70-4 area stub

This command is used to specify an area as a stub area. Use the **no** form of this 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 **no area** *AREA-ID* **stub** command removes all stub related settings associated with the area. Use this command on all routers in the stub area.

Use the **no-summary** parameter to specify the area as a total stubby area. Routers in the area do not require knowing 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 3 stub
Switch(config-router)#
```

70-5 area virtual-link

This command is used to configure the link through a non-backbone area that is physically separated from the backbone area. Use the **no** form of this 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]] [hello-interval** *SECONDS***] [dead-interval** *SECONDS***] [authentication-key** *PASSWORD* **| message-digest-key** *KEY-ID* **md5** *KEY***]**

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[authentication] [hello-interval] [dead-interval] [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 this parameter is 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 this parameter is 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* **md5** *KEY*	(Optional) Specifies an up to 16 bytes long MD key for MD5 message digest authentication.

Default

By default, no OSPF virtual link is defined.

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 hello-interval 5 dead-interval 10
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
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)#
```

70-6 clear ip ospf

This command is used to restart the IPv4 OSPF process.

clear ip ospf process

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

When OSPF processes are cleared, the OSPF routing database will be cleared and OSPF processes are restarted.

Example

This example shows how to clear OSPF processes.

```
Switch#clear ip ospf process
Switch#
```

70-7 compatible rfc3509

This command is used to implement the OSPF Area Border Router (ABR) behavior as defined in RFC 3509. Use the **no** form of this command to disable the option.

compatible rfc3509

no compatible rfc3509

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Though the definition of the ABR in the OSPF specification does not require a router with multiple attached areas to have a backbone connection, it is actually necessary to provide successful routing to the inter-area and external destinations. If this requirement is not met, all traffic destined for the areas not connected to such an ABR or out of the OSPF domain, is dropped. The alternative implementation (RFC 3509) is provided to resolve this situation.

Example

This example shows how to enable the alternative implementation of OSPF ABR.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#compatible rfc3509
Switch(config-router)#
```

70-8 compatible rfc1583

This command is used to configure the RFC 1583-compatible option in the RFC2328. Use the **no** form of this command to disable the option.

compatible rfc1583

no compatible rfc1583

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

In RFC2328, there is a new preference comparison method for AS external routes. The backward compatible is allowed by enabling the RFC1583 Compatibility option.

Example

This example shows how to enable the RFC 1583-compatible option in the RFC2328.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#compatible rfc1583
Switch(config-router)#
```

70-9 default-information originate

This command is used to advertise a default route to the OSPF routing domain. Use **no** command to disable the function.

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 routing table.
metric *METRIC-VALUE*	(Optional) Specifies the cost associated the generated default route. If this parameter is not specified, the default metric cost is 1. The valid value is from 1 to 65535.

Default

By default, this feature is disabled.

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 routing table.

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)#
```

70-10 default-metric

This command is used to configure the default metric value for the routing protocol. Use the **no** form of this 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** 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)#
```

70-11 distance ospf

This command is used to configure the distance for specific OSPF routes. Use the **no** form of the command to remove the assignment.

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 1 and 255.

Default

By default, the Intra-area distance is 80.

By default, the Inter-area distance is 90.

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.

In general, the higher the value is, the lower the rating of trustworthiness is.

Example

This example shows how to configure the distance of external routes with type-1 metric to 50.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#distance ospf external-1 50
Switch(config-router)#
```

70-12 host area

This command is used to configure a stub host entry belonging to a particular area. Use the **no** form of this 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 *COST*	(Optional) Specifies cost for the stub host entry. The range is from 1 to 65535. The default value is 1.

Default

By default, no host is configured.

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
Switch(config-router)#host 172.16.10.100 area 1
Switch(config-router)#
```

70-13 ip ospf authentication

This command is used to define the authentication mode for OSPF. Use the **no** form of this 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, 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 authentication message-digest
Switch(config-if)#
```

70-14 ip ospf authentication-key

This command is used to specify an OSPF authentication password for the authentication with the neighboring routers. Use the **no** form of this 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.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ip ospf authentication
Switch(config-if)#ip ospf authentication-key test
Switch(config-if)#
```

70-15 ip ospf cost

This command is used to specify the cost of sending packets on an interface. Use the **no** form of this command to remove the assignment.

ip ospf cost *COST*

no ip ospf cost

Parameters

COST	Specifies the value of the link-state metric. The range of value is from 1 to 65535.

Default

By default, the value is 1.

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.

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)#
```

70-16 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. Use the **no** form of this command to revert to the default setting.

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

By default, this value 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)#
```

70-17 ip ospf hello-interval

This command is used to specify the interval between hello packets. Use the **no** form of this command to revert to the default setting.

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)#
```

70-18 ip ospf message-digest-key

This command is used to configure the MD5 digest key for OSPF MD5 authentication. Use the **no** form of this 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.

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)#
```

70-19 ip ospf network

This command is used to configure the OSPF network type. Use the **no** form of this command to revert to the default setting.

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

By default, the network type is broadcast.

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)#
```

70-20 ip ospf priority

This command is used to configure the router priority that is used to determine the designated router for the network. Use the **no** form of this command to revert to the default setting.

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)#
```

70-21 log-adjacency-changes

This command is used to enable the sending of syslog messages when the OSPF neighbors go up or down. Use the **no** form of this command to disable the option.

log-adjacency-changes [detail]

no log-adjacency-changes [detail]

Parameters

detail	(Optional) Specifies to send syslog messages for all changes of the OSPF neighbor state.

Default

By default, this option is enabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of syslog messages when the OSPF neighbors go up or down.

Example

This example shows how to enable the sending of syslog messages when the OSPF neighbor state changes.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#log-adjacency-changes detail
Switch(config-router)#
```

70-22 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** form of this 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 enable OSPF routing with the specified area ID on interfaces. The interface that matches the specific network address should be enabled to run OSPF.

Example

This example shows how to enable OSPF on an interface in area 1.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#network 10.0.0.0 255.0.0.0 area 1
Switch(config-router)#
```

70-23 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.

Example

This example shows how to remove area 3 and all options associated with the area 3.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#no area 3
Switch(config-router)#
```

70-24 passive-interface

This command is used to disable the sending and receiving of the OSPF routing updates on an interface. Use the **no** form of this command to enable the sending and receiving of routing updates.

passive-interface {default | *INTERFACE-ID***}**

no passive-interface {default | *INTERFACE-ID***}**

Parameters

default	Specifies that all interfaces will operate in the passive mode.
INTERFACE-ID	Specifies the ID of the interface that will operate in the passive mode.

Default

By default, no interface is configured to operate in the passive mode.

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)#
```

70-25 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: **connected**, **rip**, or **static**.
metric *METRIC-VALUE*	(Optional) Specifies a metric for the redistributed routes. The valid value is from 1 to 16777214.
metric-type *TYPE-VALUE*	(Optional) Specifies the metric type of the external route being redistributed into the OSPF routing domain. It can be one of two values: **1:** Specifies to use the OSPF external metric type 1. **2:** Specifies to use the OSPF external metric type 2. If a metric type is not specified, the Switch will adopt a type 2.
route-map *MAP-NAME*	(Optional) Specifies the route map that filters the imported routes from this source routing protocol. If this parameter is 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.

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.

Use the **redistribute** or the **default-information originate** command only on the ASBR

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.

Example

This example shows how RIP routes are redistributed into an OSPF domain.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#redistribute rip metric 100
Switch(config-router)#
```

70-26 router ospf

This command is used to configure the OSPF routing process. Use the **no** form of this command to remove the OSPF routing process.

router ospf

no router ospf

Parameters

None.

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)#
```

70-27 router-id

This command is used to specify a router ID for the OSPF process. Use the **no** form of this command to revert to the default setting.

router-id *ROUTER-ID*

no router-id

Parameters

ROUTER-ID	Specifies the router ID in the IPv4 address format.

Default

By default, the router ID is automatically selected.

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.

Example

This example shows how to configure the router ID to 10.10.10.60.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#router-id 10.10.10.60
Switch(config-router)#
```

70-28 show ip ospf

This command is used to display general information about the OSPF routing process.

show ip ospf

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display general OSPF protocol information.

Example

This example shows how to display general OSPF protocol information.

```
Switch#show ip ospf

OSPF Routing Process 1
  Operational Router ID 10.90.90.90
  Process uptime is 0DT3H13M49S
  Conforms to RFC2328, and RFC1583 Compatibility flag is disabled
  SPF schedule Hold time between two SPFs 3 secs
  Number of external LSA 0. Checksum Sum 0x0
  Number of LSA originated 0
  Number of LSA received 0
  Number of current LSA 0
  LSDB database overflow limit is 49152
  Number of areas attached to this router: 2
    Area 0.0.0.0 (BACKBONE)
        Number of interface in this area is 0, active interface number is 0
        SPF algorithm executed 3 times
        Number of LSA 0
    Area 0.0.0.1
        Number of interface in this area is 1, active interface number is 0
        SPF algorithm executed 3 times
        Number of LSA 0
        Summarize range 192.168.0.0/16 advertise

Switch#
```

70-29 show ip ospf database

This command is used to display the database summary information for OSPF.

show ip ospf database

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the database summary information for OSPF.

Example

This example shows how to display the database summary information for OSPF.

```
Switch#show ip ospf database

          OSPF Router with ID (1.1.1.1)

              Router Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Link Count
1.1.1.1         1.1.1.1         376  0x80000003 0x7AB2 1
10.1.1.100      10.1.1.100      316  0x80000008 0xA63D 1

              Net Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum
10.1.1.1        1.1.1.1         381  0x80000001 0xE6ED

              Summary Link States (Area 0.0.0.0)

Link ID         ADV Router      Age  Seq#       CkSum  Route
50.1.1.0        10.1.1.100      317  0x80000002 0x2099 50.1.1.0/24
50.1.2.0        10.1.1.100      317  0x80000002 0x15A3 50.1.2.0/24
50.1.3.0        10.1.1.100      317  0x80000002 0xAAD  50.1.3.0/24

              AS External Link States

Link ID         ADV Router      Age  Seq#       CkSum  Route                Tag
50.1.2.0        10.1.1.100      316  0x80000002 0x9A5  E1 50.1.2.0/24       0
50.1.3.0        10.1.1.100      316  0x80000002 0xFDAF E1 50.1.3.0/24       0
50.1.4.0        10.1.1.100      316  0x80000002 0xF2B9 E1 50.1.4.0/24       0
50.1.5.0        10.1.1.100      317  0x80000002 0x6BBF E2 50.1.5.0/24       0
100.1.1.0       1.1.1.1         415  0x80000002 0x7DBE E2 100.1.1.0/24      0
100.1.2.0       1.1.1.1         415  0x80000002 0x72C8 E2 100.1.2.0/24      0
100.1.3.0       1.1.1.1         415  0x80000002 0x67D2 E2 100.1.3.0/24      0

Total Entries: 13
Switch#
```

70-30 show ip ospf database adv-router

This command is used to display all of the LSAs generated by the advertising router.

show ip ospf database adv-router *ROUTER-ID*

Parameters

ROUTER-ID	Specifies the router ID in IPv4 address format.

Default

None.

Command Mode

User/Privileged EXEC 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 adv-router 10.1.1.100

            OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.0)

  LS age: 476
  Options: 0x0 (*|-|-|-|-|-|-|-)
  Flags: 0x3 ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.1.1.100
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000008
  Checksum: 0xA63D
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.100
      Number of TOS metrics: 0
       TOS 0 Metric: 10

                Summary Link States (Area 0.0.0.0)

  LS age: 477
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.1.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x2099
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

  LS age: 478
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.2.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x15A3
  Length: 28
```

```
Network Mask: /24
      TOS: 0 Metric: 0

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: summary-LSA (summary Network Number)
Link State ID: 50.1.3.0 (summary Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0xAAD
Length: 28
Network Mask: /24
      TOS: 0 Metric: 0

              AS External Link States

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-external-LSA
Link State ID: 50.1.2.0 (External Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0x9A5
Length: 36
Network Mask: /24
      Metric Type: 1
      TOS: 0
      Metric: 0
      Forward Address: 0.0.0.0
      External Route Tag: 0

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-external-LSA
Link State ID: 50.1.3.0 (External Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0xFDAF
Length: 36
Network Mask: /24
      Metric Type: 1
      TOS: 0
      Metric: 0
      Forward Address: 0.0.0.0
      External Route Tag: 0

LS age: 478
Options: 0x0 (*|-|-|-|-|-|-|-)
LS Type: AS-external-LSA
Link State ID: 50.1.4.0 (External Network Number)
Advertising Router: 10.1.1.100
LS Seq Number: 0x80000002
Checksum: 0xF2B9
Length: 36
Network Mask: /24
      Metric Type: 1
      TOS: 0
```

```
        Metric: 0
        Forward Address: 0.0.0.0
        External Route Tag: 0

  LS age: 479
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-external-LSA
  Link State ID: 50.1.5.0 (External Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x6BBF
  Length: 36
  Network Mask: /24
        Metric Type: 2 (Larger than any link state path)
        TOS: 0
        Metric: 0
        Forward Address: 0.0.0.0
         External Route Tag: 0

Total Entries: 8
Switch#
```

70-31 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 database asbr-summary [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.
adv-router	(Optional) Specifies to display all the ABSR summary LSAs of the specified router.
IP-ADDRESS	(Optional) Specifies the advertise router IP address.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the ASBR summary LSAs.

Example

This example shows how to display information about the ASBR summary LSAs.

```
Switch#show ip ospf database asbr-summary

            OSPF Router with ID (1.1.1.1)

                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#
```

70-32 show ip ospf database external

This command is used to display information about the external LSAs.

show ip ospf database external [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.
adv-router	(Optional) Specifies to display all the external LSAs of the specified router.
IP-ADDRESS	(Optional) Specifies the advertise router IP address.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information about the external LSAs.

Example

This example shows how to display information about the external LSAs.

```
Switch#show ip ospf database external

            OSPF Router with ID (1.1.1.1)

                AS External Link States

  LS age: 631
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: AS-external-LSA
  Link State ID: 50.1.2.0 (External Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000002
  Checksum: 0x9A5
  Length: 36
  Network Mask: /24
        Metric Type: 1
        TOS: 0
        Metric: 0
        Forward Address: 0.0.0.0
        External Route Tag: 0

Total Entries: 1
Switch#
```

70-33 show ip ospf database network

This command is used to display information about the network LSAs.

show ip ospf database network [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.
adv-router	(Optional) Specifies to display all the network LSAs of the specified router.
IP-ADDRESS	(Optional) Specifies the advertise router IP address.

Default

None.

Command Mode

User/Privileged EXEC 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

            OSPF Router with ID (1.1.1.1)

                Net Link States (Area 0.0.0.0)

  LS age: 1024
  Options: 0x2 (*|-|-|-|-|-|E|-)
  LS Type: network-LSA
  Link State ID: 10.1.1.1 (address of Designated Router)
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0xE6ED
  Length: 32
  Network Mask: /24
        Attached Router: 1.1.1.1
        Attached Router: 10.1.1.100

Total Entries: 1
Switch#
```

70-34 show ip ospf database nssa-external

This command is used to display information about the NSSA-external LSAs.

show ip ospf database nssa-external [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.
adv-router	(Optional) Specifies to display all the NSSA-external LSAs of the specified router.
IP-ADDRESS	(Optional) Specifies the advertise router IP address.

Default

None.

Command Mode

User/Privileged EXEC 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

            OSPF Router with ID (30.1.1.1)

                NSSA-external Link States (Area 0.0.0.61)

  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#
```

70-35 show ip ospf database self-originate

This command is used to display LSAs generated by the local router.

show ip ospf database self-originate

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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

            OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.0)

  LS age: 38
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 ASBR
  LS Type: router-LSA
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000004
  Checksum: 0x78B3
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.1
      Number of TOS metrics: 0
       TOS 0 Metric: 1

Total Entries: 1
Switch#
```

70-36 show ip ospf database router

This command is used to display information about the router LSAs.

show ip ospf database router [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.
adv-router	(Optional) Specifies to display all the router LSAs of the specified router.
IP-ADDRESS	(Optional) Specifies the advertise router IP address.

Default

None.

Command Mode

User/Privileged EXEC 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

            OSPF Router with ID (1.1.1.1)

                Router Link States (Area 0.0.0.0)

  LS age: 246
  Options: 0x2 (*|-|-|-|-|-|E|-)
  Flags: 0x2 ASBR
  LS Type: router-LSA
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000004
  Checksum: 0x78B3
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.1
      Number of TOS metrics: 0
        TOS 0 Metric: 1

  LS age: 106
  Options: 0x0 (*|-|-|-|-|-|-|-)
  Flags: 0x3 ABR ASBR
  LS Type: router-LSA
  Link State ID: 10.1.1.100
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000009
  Checksum: 0xA43E
  Length: 36
  Number of Links: 1
    Link connected to a Transit Network
     (Link ID) Designated Router address: 10.1.1.1
     (Link Data) Router Interface address: 10.1.1.100
      Number of TOS metrics: 0
        TOS 0 Metric: 10

Total Entries: 2
Switch#
```

70-37 show ip ospf database stub

This command is used to display information about the LSAs in the stub and NSSA areas.

show ip ospf database stub [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.

adv-router	(Optional) Specifies to display all the LSAs of the specified router in the stub and NSSA areas.
IP-ADDRESS	(Optional) Specifies the advertise router IP address.

Default

None.

Command Mode

User/Privileged EXEC 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

           OSPF Router with ID (1.1.1.1)

               Router Link States (Area 0.0.0.2)

  LS age: 593
  Options: 0x0 (*|-|-|-|-|-|-|-)
  Flags: 0x13 ABR ASBR
  LS Type: router-LSA
  Link State ID: 1.1.1.1
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000003
  Checksum: 0x3BEF
  Length: 36
  Number of Links: 1
    Link connected to Stub Network
     (Link ID) Network/subnet number: 10.1.1.0
     (Link Data) Network Mask: 255.255.255.0
      Number of TOS metrics: 0
       TOS 0 Metric: 1

               Summary Link States (Area 0.0.0.2)

  LS age: 632
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 20.1.1.0 (summary Network Number)
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0x59EA
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 1

  LS age: 632
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 30.1.1.0 (summary Network Number)
  Advertising Router: 1.1.1.1
  LS Seq Number: 0x80000001
  Checksum: 0xD663
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 1

Total Entries: 3
Switch#
```

70-38 show ip ospf database summary

This command is used to display information about the summary LSAs.

show ip ospf database summary [*LINK-STATE-ID* **| self-originate | adv-router** *IP-ADDRESS***]**

Parameters

LINK-STATE-ID	(Optional) Specifies the link state ID (as an IP address).
self-originate	(Optional) Specifies the self-originated link states.
adv-router	(Optional) Specifies to display all the summary LSAs of the specified router.
IP-ADDRESS	(Optional) Specifies the advertise router IP address

Default

None.

Command Mode

User/Privileged EXEC 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

            OSPF Router with ID (1.1.1.1)

                Summary Link States (Area 0.0.0.0)

  LS age: 223
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.1.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000003
  Checksum: 0x1E9A
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

  LS age: 223
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.2.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000003
  Checksum: 0x13A4
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

  LS age: 223
  Options: 0x0 (*|-|-|-|-|-|-|-)
  LS Type: summary-LSA (summary Network Number)
  Link State ID: 50.1.3.0 (summary Network Number)
  Advertising Router: 10.1.1.100
  LS Seq Number: 0x80000003
  Checksum: 0x8AE
  Length: 28
  Network Mask: /24
        TOS: 0 Metric: 0

Total Entries: 3
Switch#
```

70-39 show ip ospf interface

This command is used to display interface information for OSPF.

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display interface information for OSPF. If no interface 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

vlan1 is up, line protocol is up
  Internet Address: 10.1.1.1/24, Area 0.0.0.0
  Process ID 1 Router ID 1.1.1.1, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.1, Interface Address 10.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

vlan100 is up, line protocol is up
  Internet Address: 20.1.1.1/24, Area 0.0.0.0
  Process ID 2 Router ID 1.1.1.2, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.2, Interface Address 20.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

vlan101 is up, line protocol is up
  Internet Address: 30.1.1.1/24, Area 0.0.0.0
  Process ID 3 Router ID 1.1.1.3, Network Type BROADCAST, Cost: 1
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 1.1.1.3, Interface Address 30.1.1.1
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

Total Entries: 3
Switch#
```

70-40 show ip ospf neighbor

This command is used to display information of OSPF neighbors.

show ip ospf neighbor [interface *INTERFACE-ID* **|** *NEIGHBOR-ID***] [detail]**

Parameters

interface *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.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information of OSPF neighbors. If no interface 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           Address         Interface
---------------- ----- --------------- --------------- ------------
10.1.1.100       0     Full/DROther    10.1.1.100      vlan1
20.1.1.100       0     Full/DROther    20.1.1.100      vlan100
30.1.1.100       0     Full/DROther    30.1.1.100      vlan101

Total Entries: 3
Switch#
```

This example shows how to display detail information of OSPF neighbors.

```
Switch#show ip ospf neighbor detail

Neighbor 10.1.1.100, interface  address 10.1.1.100
    In the area 0.0.0.0 via interface vlan1
    Neighbor priority is 0, State is Full, 6 state change
    DR is 10.1.1.1, BDR is 0.0.0.0
    Options: 0x2 (*|-|-|-|-|-|E|-)

Neighbor 20.1.1.100, interface  address 20.1.1.100
    In the area 0.0.0.0 via interface vlan100
    Neighbor priority is 0, State is Full, 6 state change
    DR is 20.1.1.1, BDR is 0.0.0.0
    Options: 0x2 (*|-|-|-|-|-|E|-)

Neighbor 30.1.1.100, interface  address 30.1.1.100
    In the area 0.0.0.0 via interface vlan101
    Neighbor priority is 0, State is Full, 6 state change
    DR is 30.1.1.1, BDR is 0.0.0.0
    Options: 0x2 (*|-|-|-|-|-|E|-)

Total Entries: 3
Switch#
```

70-41 show ip ospf virtual-links

This command is used to display virtual link information.

show ip ospf virtual-links

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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 2.2.2.2 is down, Process ID 1
  Transit area 0.0.0.1
  Transmit Delay is 1 sec, State DOWN
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Current Authentication Type: none

Total Entries: 1
Switch#
```

70-42 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#
```

70-43 debug ip ospf neighbor

This command is used to turn on the OSPF neighbor state debug switch. Use the **no** form of this 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
```

70-44 debug ip ospf interface

This command is used to turn on the OSPF interface state debug switch. Use the **no** form of this 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
```

70-45 debug ip ospf log

This command is used to enable the router to send OSPF syslog messages. Use the **no** form of this command to disable the router to send OSPF syslog messages.

debug ip ospf log

no debug ip ospf log

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 enable or disable the router to send OSPF syslog messages.

Example

This example shows how to enable the router to send OSPF syslog messages.

```
Switch#debug ip ospf log
#60    2018-04-03 11:26:32 INFO(6) OSPF-6-INTFSTATECHANGE: OSPF interface vlan1 changed state
to Up.
#61    2018-04-03 11:26:34 NOTI(5) OSPF-5-NBRLOADINGTOFULL: OSPF nbr 2.2.2.2 on interface
vlan1 changed state from Loading to Full.
Switch#
```

70-46 debug ip ospf lsa-originating

This command is used to turn on the OSPF LSA originating debug switch. Use the **no** form of this 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 LSA originating 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
Build Router LSA id 100.1.1.2 for area 0.0.0.0 seq 80000001 tic 10 proc_id 1
Switch#
```

70-47 debug ip ospf lsa-flooding

This command is used to turn on the OSPF LSA flooding debug switch. Use the **no** form of this 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
```

70-48 debug ip ospf packet-receiving

This command is used to turn on the OSPF packet receiving debug switch. Use the **no** form of this 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
Received a Hello packet from addr 10.1.1.2 at interface 10.90.90.90 tic 100
Received a Hello packet from addr 100.1.1.2 at interface 100.90.90.90 tic 102
Switch#
```

70-49 debug ip ospf packet-transmitting

This command is used to turn on the OSPF packet transmitting debug switch. Use the **no** form of this 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
Send out a Hello on interface 10.1.1.1 dst 224.0.0.5 tic 200
Send out a Hello on interface 100.1.1.1 dst 224.0.0.5 tic 220
Switch#
```

70-50 debug ip ospf spf

This command is used to turn on the OSPF SPF calculation debug switch. Use the **no** form of this 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
Running SPF-intra for area 0.0.0.0 tic 300  proc_id 1
SPF-intra calculation completed tic 310
Switch#
```

70-51 debug ip ospf timer

This command is used to turn on the OSPF timer debug switch. Use the **no** form of this 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
Start Hello timer at interface 10.90.90.90 tic 20
Wait timer expired at interface 10.90.90.90 tic 100
Switch#
```

70-52 debug ip ospf virtual-link

This command is used to turn on the OSPF virtual link debug switch. Use the **no** form of this 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.

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
Virtual link up transit area 1.1.1.1 vnbr 3.3.3.3 tic 260
Switch#
```

70-53 debug ip ospf route

This command is used to turn on the OSPF route debug switch. Use the **no** form of this 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
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 proc_id 1
Switch#
```

70-54 debug ip ospf redistribution

This command is used to turn on the OSPF redistribution debug switch. Use the **no** form of this 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
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
Switch#
```

70-55 debug ip ospf show counter

This command is used to display OSPF statistic counters.

debug ip ospf show counter [packet | neighbor | spf]

Parameters

packet	(Optional) Specifies to display the OSPF packet counter.
neighbor	(Optional) Specifies to display the OSPF neighbor counter.
spf	(Optional) Specifies to display 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 display 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#
```

70-56 debug ip ospf clear counter

This command is used to reset OSPF statistic counters.

debug ip ospf clear counter [packet | neighbor | spf]

Parameters

packet	(Optional) Specifies to reset the OSPF packet counter.
neighbor	(Optional) Specifies to reset the OSPF neighbor counter.
spf	(Optional) 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#
```

70-57 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 display detailed information about Router LSAs.

```
Switch#debug ip ospf show database rt-link

OSPF Phase2 RT Link (Process ID 1):

===========
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#
```

70-58 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 (Process ID 1):

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#
```

70-59 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 (Process ID 1):

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

OSPF ASE Table (Process ID 1):

IP                  Nexthop          State Type Tag
------------------  ---------------  ----- ---- ---------------
1.1.1.0/24          0.0.0.0          ON    2    0.0.0.0

Switch#
```

70-60 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 (Process ID 1):

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#
```

71. Open Shortest Path First Version 3 (OSPFv3) Commands

71-1 area default-cost

This command is used to set the summary-default cost of a stub area. Use the **no** form of this command to disable this function.

area *AREA-ID* **default-cost** *COST*

no area *AREA-ID* **default-cost**

Parameters

AREA-ID	Specifies the identifier of the area. 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)#
```

71-2 area range

This command is used to consolidate and summarize routes at an area boundary. Use the **no** form of this command to disable this function.

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 an inter-area prefix LSA for the specified address range.
not-advertise	(Optional) Specifies to suppress the advertising of inter-area prefix LSAs. Component routes are still hidden behind it.

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)#
```

71-3 area stub

This command is used to define an area as a stub area. Use the **no** form of this command to disable this function.

area *AREA-ID* **stub [no-summary]**

no area *AREA-ID* **stub [no-summary]**

Parameters

AREA-ID	Specifies the identifier of the area. It can be specified as an IPv4 address.
no-summary	(Optional) Specifies to prevent an ABR from sending inter-area prefix LSAs into the stub area.

Default

By default, this option is disabled.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The **no area** *AREA-ID* **stub** command removes all stub related settings associated with the area. The area becomes a normal area. Use this command on all routers in the stub area.

Use the **no-summary** parameter to specify the area as a total stubby area when routers in the area do not require knowing the inter-area routes except the default inter-area route.

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)#
```

71-4 area virtual-link

This command is used to configure a virtual link through a non-backbone area that is physically separated from the backbone area. Use the **no** form of this command to remove a virtual link or reset the specific parameter to the default value.

area *AREA-ID* **virtual-link** *ROUTER-ID* **[hello-interval** *SECONDS***] [dead-interval** *SECONDS***] [transmit-delay** *SECONDS***] [retransmit-interval** *SECONDS***] [instance** *INSTANCE-ID***]**

no area *AREA-ID* **virtual-link** *ROUTER-ID* **[hello-interval] [dead-interval] [transmit-delay] [retransmit-interval]**

Parameters

AREA-ID	Specifies the identifier of the area. 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.
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.
instance-id *INSTANCE-ID*	(Optional) Specifies the instance identifier.

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.

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)#
```

71-5 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)#
```

71-6 clear ipv6 ospf

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

Privileged EXEC Mode.

Command Default Level

Level: 12.

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 all the OSPF processes.

```
Switch#clear ipv6 ospf process
Switch#
```

71-7 default-metric

This command is used to set the default metric for IPv6 OSPF. Use the **no** form of this command to revert to the default setting.

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** 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)#
```

71-8 distance ospf

This command is used to configure the distance for specific OSPF routes. Use the **no** form of this command to revert 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)#
```

71-9 ipv6 ospf area

This command is used to configure an area of an OSPF process on an interface. Use the **no** form of this command to disable OSPF routing for the interfaces defined.

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 this parameter is 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)#
```

71-10 ipv6 ospf cost

This command is used to explicitly specify the cost of sending a packet on an interface. Use the **no** form of this command to revert to the default setting.

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, this value is 10.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Set the metric manually using the **ipv6 ospf cost** command. Using the **auto-cost reference-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)#
```

71-11 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. Use the **no** form of this command to revert to the default setting.

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)#
```

71-12 ipv6 ospf hello-interval

This command is used to specify the interval between hello packets that the software sends on the interface. Use the **no** form of this command to revert to the default setting.

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)#
```

71-13 ipv6 ospf priority

This command is used to set the router priority, which helps determine the designated router for this network. Use the **no** form of this command to revert to the default setting.

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.

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)#
```

71-14 ipv6 ospf retransmit-interval

This command is used to specify the time between LSA retransmissions for adjacencies belonging to the interface. Use the **no** form of this command to revert to the default setting.

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 value is from 1 to 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)#
```

71-15 ipv6 ospf transmit-delay

This command is used to set the estimated time required to send a link-state update packet on the interface. Use the **no** form of this command to revert to the default setting.

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 value is from 1 to 65535.

Default

The default interval is 1 second.

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)#
```

71-16 ipv6 router ospf

This command is used to configure an IPv6 OSPF routing process and enter the Router Configuration mode. Use the **no** form of this command to remove an OSPF routing process.

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 specify the ID for the IPv6 OSPF routing process as 1 and enter the Router Configuration mode.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#
```

71-17 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)#
```

71-18 passive-interface

This command is used to configure the specified network interface or all interfaces as the passive interface. Use the **no** form of this command to revert to the default setting.

passive-interface {default | *INTERFACE-ID***}**

no passive-interface {default | *INTERFACE-ID***}**

Parameters

default	Specifies that all interfaces will operate in the passive mode.
INTERFACE-ID	Specifies the ID of the interface that will operate in the passive mode.

Default

By default, no interface is configured to operate in the passive mode.

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)#
```

71-19 redistribute

This command is used to redistribute routes from other routing domain into IPv6 OSPF routing domain. Use the **no** form of this 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**, and **rip**.
metric *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.
metric-type *TYPE-VALUE*	(Optional) Specifies the metric type of the external route being redistributed into the IPv6 OSPF routing domain. It can be one of two values: **1:** Specifies to use the IPv6 OSPF external metric type 1. **2:** Specifies to use the IPv6 OSPF external metric type 2. If a metric type is not specified, the Switch will adopt a type 2.

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** command 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, 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 prefix is learned through IPv6 RIP.

```
Switch#configure terminal
Switch(config)#ipv6 router ospf 1
Switch(config-rtr)#redistribute rip
Switch(config-rtr)#
```

71-20 router-id

This command is used to specify a router ID for the OSPF process. Use the **no** form of this command to revert to the default setting.

router-id *ROUTER-ID*

no router-id

Parameters

ROUTER-ID	Specifies the router ID in the IPv4 address format.

Default

By default, the router ID is automatically selected.

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)#
```

71-21 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/Privileged EXEC 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 1" with ID 107.100.0.1
  Process uptime is  0DT1H3M50S
  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 (with default metric 20) from,
     rip with metric 0 with metric-type 2
  SPF schedule delay 5 secs, Hold time between SPFs 10 secs
  Number of LSA originated 69
  Number of LSA received 200
  Number of areas in this router is 6
    Area 0.0.0.0 (BACKBONE) (active)
        Number of interfaces in this area is 2 active interface number is 1
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 3 times
        Number of LSA 30. Checksum Sum 0xf521c
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.1
        Number of interfaces in this area is 0 active interface number is 0
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x0
```

```
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.11 (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 16. Checksum Sum 0x80fcd
        Number of Unknown LSA 0
        Area ranges are
    Area 0.0.0.107 (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 14. Checksum Sum 0x78472
        Number of Unknown LSA 0
        Area ranges are
    Area 1.1.1.100
        Number of interfaces in this area is 0 active interface number is 0
        Number of fully adjacent virtual neighbors through this area is 0
        It is a stub area
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x0
        Number of Unknown LSA 0
        Area ranges are
    Area 1.1.1.101
        Number of interfaces in this area is 0 active interface number is 0
        Number of fully adjacent virtual neighbors through this area is 0
        SPF algorithm executed 0 times
        Number of LSA 0. Checksum Sum 0x0
        Number of Unknown LSA 0
        Area ranges are

Switch#
```

71-22 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/Privileged EXEC 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#
```

71-23 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/Privileged EXEC 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

Total Entries: 36
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#
```

71-24 show ipv6 ospf interface

This command is used to display OSPF-related interface information.

show ipv6 ospf [*PROCESS-ID***] interface [***INTERFACE-ID***]**

Parameters

PROCESS-ID	(Optional) Specifies the process ID. The ID of a process is used internally and should be uniquely locally assigned.
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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display interface information for OSPFv3. If no interface is specified, OSPFv3 information of all interfaces will be displayed.

Example

This example shows how to display OSPF-related interface information.

```
Switch#show ipv6 ospf interface

vlan1 is up, line protocol is up
  Link Local Address: FE80::20F:36FF:FE31:AE01/128
  Interface ID: 1
  OSPFv3 Process (1), Area 0.0.0.107 (active), Instance ID 0, MTU 1500
  Router ID 107.100.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State DR, Priority 1
  Designated Router (ID) 107.100.0.1,
    Local Address FE80::20F:36FF:FE31:AE01
  Backup Designated Router (ID) 0.0.0.0,
    Local Address ::
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Neighbor Count is 0, Adjacent neighbor count is 0
  Hello received 0 sent 535, DD received 0 sent 0
  LS-Req received 0 sent 0, LS-Upd received 0 sent 0
  LS-Ack received 0 sent 0, Discarded 0

vlan11 is up, line protocol is up
  Link Local Address: FE80::20F:36FF:FE31:AE03/128
  Interface ID: 2
  OSPFv3 Process (1), Area 0.0.0.11 (active), Instance ID 11, MTU 1500
  Router ID 107.100.0.1, Network Type BROADCAST, Cost: 10
  Transmit Delay is 1 sec, State Backup, Priority 1
  Designated Router (ID) 30.90.90.90,
    Local Address FE80::206:28FF:FED8:FE94
  Backup Designated Router (ID) 107.100.0.1,
    Local Address FE80::20F:36FF:FE31:AE03
  Timer intervals configured, Hello 10, Dead 40, Retransmit 5
  Neighbor Count is 1, Adjacent neighbor count is 1
  Hello received 587 sent 491, DD received 8 sent 6
  LS-Req received 1 sent 4, LS-Upd received 26 sent 24
  LS-Ack received 23 sent 27, Discarded 0

Total Entries: 2
Switch#
```

71-25 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display information of OSPFv3 neighbors. If no interface is specified, OSPFv3 neighbor information of all interfaces will be displayed.

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#
```

71-26 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/Privileged EXEC 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#
```

72. Packet Debug Commands

72-1 debug clear cpu counter

This command is used to clear packet counters including RX and TX of the CPU port.

debug clear cpu counter

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to clear packet counters including RX and TX of the CPU port and calculate again.

Example

This example shows how to clear packet counters of the CPU.

```
Switch#debug clear cpu counter

Success

Switch#
```

72-2 debug dump packet_in_buffer

This command is used to check received packets in buffer.

debug dump packet_in_buffer [len *LENGTH***][count** *COUNT***] [channel** *CHANNEL***]**

Parameters

len *LENGTH*	(Optional) Specifies the print buffer length of each packet in bytes. The value is from 0 to 2048.
count *COUNT*	(Optional) Specifies the packets count in each channel. The value is from 0 to 200.
channel *CHANNEL*	(Optional) Specifies the dump channel. The value is from 1 to 3.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

The command is used to check received packets in buffer. The system can buffer up to 200 packets per channel, and there are 3 channels in total for all packets. The system will prefer the lower position for the newer incoming packet. If the system is busy, the received packets will be buffered in the higher position. This can be used to check packets in the higher position for the CPU busy reason.

Example

This example shows how to dump packets in channel 2.

```
Switch#debug dump packet_in_buffer channel 2

================================================================================
Rx channel 2, base address=0x7f869ab8,total_size=432800,block_size=2148,
    block_num=200,max_alloc=20,alloc_blocks=8 print count=20(input 0)
=>7f869ac4--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 6b 76  40 00 7f 06 c7 3c 0a 5a    ..E..(kv@....<.Z
0020: 5a 0f 0a 5a 5a 5a c0 09  00 50 0f 8f b3 6e 28 49    Z..ZZZ...P...n(I
0030: 97 c7 50 10 40 de 62 71  00 00                      ..P.@.bq..
=>7f86a338--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 4c ec  40 00 7f 06 e5 c7 0a 5a    ..E..(L.@......Z
0020: 5a 0e 0a 5a 5a 5a 12 e0  00 50 6c 99 64 c8 14 05    Z..ZZZ...Pl.d...
0030: df d8 50 10 40 de cd 6a  00 00                      ..P.@..j..
=>7f86abac--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 6b 78  40 00 7f 06 c7 3a 0a 5a    ..E..(kx@....:.Z
0020: 5a 0f 0a 5a 5a 5a c0 13  00 50 0e 98 e2 09 50 39    Z..ZZZ...P....P9
0030: b8 13 50 10 3f dc ed 88  00 00                      ..P.?.....
=>7f86b420--------------------------------------------------------------------
0000: f0 7d 68 34 00 10 f0 7d  68 34 00 10 81 00 00 01    .}h4...}h4......
0010: 08 00 45 00 00 28 6b 77  40 00 7f 06 c7 3b 0a 5a    ..E..(kw@....;.Z
0020: 5a 0f 0a 5a 5a 5a c0 13  00 50 0e 98 e2 09 50 39    Z..ZZZ...P....P9
0030: b7 65 50 10 40 07 ee 0b  00 00                      .eP.@.....
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

72-3 debug show cpu counter

This command is used to display packet counters including RX and TX of the CPU port.

debug show cpu counter

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to display packet counters including RX and TX of the CPU port.

Example

This example shows how display packet counters of the CPU port.

```
Switch#debug show cpu counter

PacketType    TotalCounter     Pkt/Sec  PacketType    TotalCounter     Pkt/Sec
----------- ------RX-TX------ --RX-TX-- ----------- ------RX-TX------ --RX-TX--
UNKNOWN            0-0           0-0    1X_BPDU            0-0           0-0
STP_BPDU           0-0           0-0    GVRP_BPDU          0-0           0-0
IP              1102-936         0-0    LACP_BPDU          0-0           0-0
BPDU               0-0           0-0    ARP             2313-2           2-0
GM                 0-0           0-0    IPv6               0-0           0-0
CTP                0-0           0-0    OSPF_TIC           0-0           0-0
OSPF_ACK           0-0           0-0    OSPF_PKT           0-0           0-0
LLDP               0-0           0-0    LOOPBACK           0-0           0-0
ERPS_PDU           0-0           0-0    Tunnel_STP         0-0           0-0
Tunnel_GVRP        0-0           0-0    CISCO_MAC1         0-0           0-0
CISCO_MAC2         0-0           0-0    L2PT_MAC1          0-0           0-0
L2PT_MAC2          0-0           0-0    TUNNEL_LLDP        0-0           0-0
OSPF6_TIC          0-0           0-0    OSPF6_ACK          0-0           0-0
OSPF6_PKT          0-0           0-0    DDPv4              0-0           0-0
DDPv6              0-0           0-0    DDP_L2             0-0           0-0
Stacking           0-0           0-0    Total           3415-938         2-0



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Display Parameters

PacketType	Received packets type of each protocol.
TotalCounter	Total received and transmitted counters of CPU port.
Pkt/Sec	RX or TX rate in packets per second.

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. Use the **no** form of this command to disable policy routing on the interface.

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 the 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 does not 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 ipv6 policy route-map

This command is used to specify a route map as the routing policy on an interface. Use the **no** form of this command to disable policy routing on the interface.

ipv6 policy route-map *MAP-NAME*

no ipv6 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 ipv6-address** command in the route map to define the matching criteria for packets with specific characteristics. If the IPv6 access list is used with the **match ipv6-address** command, all of the matching criteria in the access list will be checked. The packet that matches the 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 ipv6 next-hop
- set ipv6 default next-hop
- set ipv6 precedence

Example

This example shows how to set up the routing policy to route the packets that match the IPv6 access list name “pbr-acl” to the next-hop 1001::100.

```
Switch#configure terminal
Switch(config)#route-map pbr-map permit 1
Switch(config-route-map)#match ipv6 address pbr-acl
Switch(config-route-map)#set ipv6 next-hop 1001::100
Switch(config-route-map)#exit
Switch(config)#interface vlan 1
Switch(config-if)#ipv6 policy route-map pbr-map
Switch(config-if)#
```

73-3 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/Privileged EXEC 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

Total Entries: 3
Switch#
```

73-4 show ipv6 policy

This command is used to display the route map used for policy-based routing.

show ipv6 policy

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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 ipv6 policy

Interface    Route Map
------------ ----------------
vlan1        pbr-map

Total Entries: 1
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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
vlan *VLAN-ID*	Specifies to delete the auto-learned secured entry learned with the specified VLAN.

Default

None.

Command Mode

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

interface *INTEFACE-ID*	(Optional) Specifies the ID of the interface to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
address	(Optional) Specifies to display all the secure MAC addresses, including both configured and learned entries.
vlan *VLAN-ID*	(Optional) Specifies to display port security settings for the VLAN.
.	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 on ports 1 to 3.

```
Switch#show port-security interface eth1/0/1-3

 D:Delete-on-Timeout    P:Permanent
 Interface    Max  Curr   Violation    Violation   Security  Admin   Current
 No.          No.   No.     Act.       Count           Mode  State   State
 ------------ ----- ----- -------- -------------------- -- -------- ------------
 eth1/0/1     5     2     Restrict 0                    D  Enabled  Forwarding
 eth1/0/2     10    10    Shutdown 0                    D  Enabled  Err-disabled
 eth1/0/3     10    0     Shutdown 0                    P  Disabled -

Switch#
```

74-3 snmp-server enable traps port-security

This command is used to enable the sending of SNMP notifications for port security address violations. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps port-security [trap-rate *TRAP-RATE***]**

no snmp-server enable traps port-security [trap-rate]

Parameters

trap-rate *TRAP-RATE*	(Optional) Specifies the number of traps to send per second. The range is from 0 to 1000. The default value of 31 indicates that an SNMP trap is to be generated for every security violation.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable the sending of SNMP notifications for port security address violations.

Example

This example shows how to enable the sending of traps for port security address violations and set the number of traps per second to 3.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps port-security
Switch(config)#snmp-server enable traps port-security trap-rate 3
Switch(config)#
```

74-4 switchport port-security

This command is used to configure the port security settings to restrict the number of users that are allowed to gain access rights to a port. Use the **no** form of this command to disable port security or to delete a secure MAC address.

switchport port-security [maximum *VALUE* **| violation {protect | restrict | shutdown} | mode {permanent | delete-on-timeout} | mac-address [permanent]** *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

no switchport port-security [maximum | violation | mode | mac-address [permanent] *MAC-ADDRESS* **[vlan** *VLAN-ID***]]**

Parameters

maximum *VALUE*	(Optional) Specifies to set the maximum number of secure MAC addresses allowed. If this parameter is not specified, the default value is 32. The valid range is from 0 to 3328.
protect	(Optional) Specifies to drop all packets from the insecure hosts at the port-security process level, but does not increment the security-violation count.
restrict	(Optional) Specifies to drop all packets from the insecure hosts at the port-security process level and increments the security-violation count and record the system log.
shutdown	(Optional) Specifies to shut down the port if there is a security violation and record the system log.

permanent	(Optional) Specifies that under this mode, all learned MAC addresses will not be purged out unless the user manually deletes those entries.
delete-on-timeout	(Optional) Specifies that under this mode, all learned MAC addresses will be purged out when an entry is aged out or when the user manually deletes these entries.
mac-address *MAC-ADDRESS*	(Optional) Specifies to add a secure MAC address to gain port access rights.
permanent	(Optional) Specifies to set the secure permanent configured MAC address of the port. This entry is same as the one learnt under the permanent mode.
vlan *VLAN-ID*	(Optional) Specifies a VLAN. If no VLAN is specified, the MAC address will be set with a PVID.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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), 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 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security mac-address 00-00-12-34-56-78 vlan 5
Switch(config-if)#
```

This example shows how to configure the Switch to drop all packets from the insecure hosts at the port-security process level and increment the security violation counter if a security violation is detected.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security violation restrict
Switch(config-if)#
```

74-5 switchport port-security aging

This command is used to configure the aging time for auto-learned dynamic secure addresses on an interface. Use the **no** form of this command to revert to the default setting.

switchport port-security aging {time *MINUTES* **| type {absolute | inactivity}}**

no switchport port-security aging {time | type}

Parameters

time *MINUTES*	Specifies the aging time for the auto-learned dynamic secured address on this port. Its range is from 0 to 1440 in minutes.
type	Specifies to set the aging type.
absolute	Specifies to set absolute aging type. All the secure addresses on this port age out exactly after the time specified and is removed from the secure address list. This is the default type.
inactivity	Specifies to set the inactivity aging type. The secure addresses on this port age out only if there is no data traffic from the secure source address for the specified time period.

Default

By default, the port security aging feature is disabled.

The default time is 0 minutes.

The default aging type is **absolute**.

Command Mode

Interface Configuration Mode.

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 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security aging time 1
Switch(config-if)#
```

This example shows how to configure the port security aging time type on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport port-security aging type inactivity
Switch(config-if)#
```

74-6 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 revert 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.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
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 3328. If the setting is smaller than the number of current learned entries, the command will be rejected.

Default

By default, this option is no limit.

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 over Ethernet (PoE) Commands (DGS-1520-28MP and DGS-1520-52MP Only)

75-1 poe pd description

This command is used to configure the description for the PD connected to the PoE port. Use the **no** form of this command to clear the description.

poe pd description *TEXT*

no poe pd description

Parameters

TEXT	Specifies the string that describes the PD connected to a PoE interface. The maximum length is 32 characters.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to configure a description for the PD connected to the port.

Example

This example shows how to configure the PoE PD description on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe pd description For VOIP usage
Switch(config-if)#
```

75-2 poe pd legacy-support

This command is used to enable the support of legacy PD. Use the **no** form of this command to disable it.

poe pd legacy-support

no poe pd legacy-support

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.

Use this command to enable the support of legacy PDs connected to the port. If legacy support is disabled, the system will not provide power to the legacy PDs.

Example

This example shows how to enable legacy support for PDs connected to port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe pd legacy-support
Switch(config-if)#
```

75-3 poe pd priority

This command is used to configure the priority for provisioning power to the port. Use the **no** form of this command to revert to the default setting.

poe pd priority {critical | high | low}

no poe pd priority

Parameters

critical	Specifies the PD connected to the port gains the highest priority.
high	Specifies the PD connected to the port gains the second high priority.
low	Specifies the PD connected to the port gains the lowest priority.

Default

By default, this option is set as low.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

Since the power budget is limited, as more PDs are added to the system, the power source may not be sufficient to supply the power. The PoE system enters the power critical section when the remaining power source is not enough to serve the new added PD. Whether power is supplied to the new added PD will depend on the policy configured by the **poe policy preempt** command.

If the policy preempt setting is disabled, the policy is first in first serviced. Thus, the new PD will not be serviced if the power source is running out. If the policy preempt setting is enabled, the power provisioned to PD with lower priority can be preempted in order to release power to the new connected PD with higher priority.

Example

This example shows how to configure the priority of port 3 to the first priority.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe pd priority critical
Switch(config-if)#
```

75-4 poe policy preempt

This command is used to enable disconnection of PD which is power-provisioned with lower priority in order to release the power to the new connected PD with higher priority under power shortage conditions. Use the **no** form of this command to revert to the default setting.

poe unit *UNIT-ID* **policy preempt**

no poe unit *UNIT-ID* **policy preempt**

Parameters

unit *UNIT-ID*	Specifies the stacking unit ID to be configured. This parameter is only available when the stacking mode is enabled.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Since the power budget is limited, as more PDs are added to the system, the power source may not be sufficient to supply the power. The PoE system enters the power critical section when the remaining power budget is not enough to serve the new added PD.

The **poe policy preempt** command configures whether to disconnect the PD which is powered with lower priority in order to release the power to the new connected PD with higher priority under power shortage condition. If the policy preempt setting is disabled, the policy is first in first serviced. Thus, the new PD will not be serviced if the power budget is running out.

If the policy preempt setting is enabled, the power provisioned to PD with lower priority can be preempted to release the power to the new connected PD with higher priority.

Example

This example shows how to configure the PoE system power service policy preemptive mode.

```
Switch#configure terminal
Switch(config)#poe unit 1 policy preempt
Switch(config)#
```

75-5 poe power-inline

This command is used to configure the power management mode for the PoE ports. Use the **no** form of this command to revert to the default setting.

poe power-inline {auto [max *MAX-WATTAGE*] **[time-range** *PROFILE-NAME*] **| never}**

no poe power-inline [auto {max | time-range}]

Parameters

auto	Specifies to enable the auto-detection of PDs and provision power to the PD.
max *MAX-WATTAGE*	(Optional) Specifies to set the maximum wattage of power that can be provisioned to the auto-detected PD. If this parameter is not specified, the class of the PD automatically determines the maximum wattage which can be provisioned. The valid range for maximum wattage is from 1000 mW to 30000 mW.
time-range *PROFILE-NAME*	(Optional) Specifies the name of the time-range profile to delineate the activation period.
never	Specifies to disable supplying power to PD connected to the port.

Default

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

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the port is set to **auto** mode, the port will automatically detect the PD and provision power to the PD. The user can explicitly specify a maximum wattage value which can be provisioned to the port. If the maximum wattage value is not specified, the class of the PD automatically determines the maximum wattage that can be provisioned. The PD will not be provisioned if it requests more wattage than the maximum wattage.

Use this command to also specify a time range with a port. Once a PoE port is associated with a time-range profile, it will only be activated during the time frame specified in the profile. That is, the PD will not get powered during timeframe out of the specified time range.

When the **no poe power-inline** command is issued, the power management mode will be reset to the default setting.

The specified time-range profile does not need to exist to configure the command. If the time-range profile does not exist, the command acts as if the time-range is not specified.



NOTE: If the Switch failed to supply power to the IEEE 802.3at PD (Powered Device),
(1) check if the PD connected to the port supports the IEEE 802.3at standard or
(2) manually configure the corresponding port's power limit value to 30 Watts using the **poe power-inline max 3000** command.

Example

This example shows how to enable PD detection and to automatically provide power to the PoE device plugged into port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline auto
Switch(config-if)#
```

This example shows how to configure the PoE port 3 to allow powered devices under 7000mw.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline auto max 7000
Switch(config-if)#
```

This example shows how to disable PD detection and not provide power to the PoE device plugged into port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline never
Switch(config-if)#
```

This example shows how to combine a time-range profile called "day-time" with the PoE port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#poe power-inline auto time-range day-time
Switch(config-if)#
```

75-6 poe usage-threshold

This command is used to configure the utilization threshold to record a log. Use the **no** form of this command to revert to the default setting.

poe unit *UNIT-ID* **usage-threshold** *PERCENTAGE*

no poe unit *UNIT-ID* **usage-threshold** *PERCENTAGE*

Parameters

unit *UNIT-ID*	Specifies the stacking unit ID to be configured. This parameter is only available when the stacking mode is enabled.
PERCENTAGE	Specifies the usage threshold to generate a log. The valid range is from 1 to 99. The unit is percentage.

Default

By default, this value is 99.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

When the usage threshold is configured, if the utilization of the PSE exceeds the configured threshold, the *EXCEED* log will be recorded. Once the percentage decreases and become lower than the threshold, the *RECOVER* log is recorded.

Example

This example shows how to configure the usage threshold to 50%.

```
Switch#configure terminal
Switch(config)#poe unit 1 usage-threshold 50
Switch(config)#
```

75-7 snmp-server enable traps poe

This command is used to enable the sending of PoE notifications. Use the **no** form of this command to disable sending power over Ethernet notifications.

snmp-server enable traps poe [unit *UNIT-ID***]**

no snmp-server enable traps poe [unit *UNIT-ID***]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the stacking unit ID to be configured. This parameter is only available when the stacking mode is enabled.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of PoE notifications.

Example

This example shows how to enable the sending of PoE notifications.

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

75-8 clear poe statistic

This command is used to clear the statistic counters on the port.

clear poe statistic {all | interface *INTERFACE-ID* **[, | -]}**

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

There are counters on ports to record the statistic and they can be shown by entering the **show poe power-inline statistics** command. Use this command to clear all the counter values on the port.

Example

This example shows how to clear statistics on port 3.

```
Switch#clear poe statistic interface eth1/0/3
Switch#
```

75-9 show poe power-inline

This command is used to the PoE status for the specified PoE port or for all PoE ports in the switch system.

show poe power-inline [*INTERFACE-ID* **[, | -]] {status | configuration | statistics | measurement | lldp-classification}**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed. If no interface is specified, all PoE interfaces will be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
status	Specifies to display the port PoE status.
configuration	Specifies to display the port configuration information.
statistics	Specifies to display the port error counters.
measurement	Specifies to display the port voltage, current, consumed power, and temperature.
lldp-classification	Specifies to display the data link layer classification using information of power via MDI TLV.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the PoE status of ports, power inline configuration status, statistic counters, the measurement result, and the data link layer classification information. Only the PoE capable interfaces are displayed.

Example

This example shows how to display the PoE power inline status on ports 1 to 8.

```
Switch#show poe power-inline eth1/0/1-8 status

Interface   State      Class   Max(W) Used(W) Description
------------------------------------------------------------------------------
eth1/0/1    delivering class-1 4      3.4     IP-camera-1
eth1/0/2    delivering class-2 10     6.3     1234567890
eth1/0/3    delivering class-3 15.4   13.0
eth1/0/4    delivering class-3 15.4   1.4     access123
eth1/0/5    searching  n/a     0.0    0.0
eth1/0/6    searching  n/a     0.0    0.0
eth1/0/7    searching  n/a     0.0    0.0
eth1/0/8    searching  n/a     0.0    0.0

Faulty code
[1] MPS (Maintain Power Signature) Absent
[2] PD short
[3] Overload
[4] Power Denied
[5] Thermal Shutdown
[6] Startup Failure
[7] Classification Failure

Switch#
```

Display Parameters

Interface	The PoE interface ID.
State	The port status can be of the following: **Disabled:** The PSE function is disabled. **Searching:** The remote PD is not connected. **Requesting:** The remote PD is inserted, but the PSE does not provide power yet. **Delivering:** The remote PD is now powering by PoE system. **Faulty[X]:** The device detection or a powered device is in a faulty state. X is the error code number. • **[1]** - MPS (Maintain Power Signature) Absent. • **[2]** - PD Short. • **[3]** - Overload. • **[4]** - Power Denied. • **[5]** - Thermal Shutdown. • **[6]** - Startup Failure. • **[7]** - Classification Failure(IEEE 802.3at).
Class	The IEEE classification: N/A or a value from IEEE class 0 to 4.
Max(W)	The maximum amount of power could be allocated to the powered device in watts.
Used(W)	The amount of power is currently allocated to PoE ports in watts.
Description	The configured description of the connected PD.

Example

This example shows how to display the PoE power inline configuration on ports 1 to 6.

```
Switch#show poe power-inline eth1/0/1-6 configuration

Interface Admin   Priority  Legacy-Support  Time-Range
-----------------------------------------------------------------------
eth1/0/1  auto    low       disabled
eth1/0/2  auto    low       disabled
eth1/0/3  auto    low       disabled
eth1/0/4  auto    critical  enabled         day-time
eth1/0/5  auto    low       disabled
eth1/0/6  auto    low       disabled

Switch#
```

Display Parameters

Interface	The PoE interface ID.
Admin	The user configured mode can be of the following: **Auto:** The powered device will be automatically detected and maximum power is based on the detection result. **Auto(M):** The powered device will be automatically detected and maximum power is the user configured value. **Never:** The powered device will not be detected, and no power to the port.
Priority	The priority used to prioritize the service order when power constrain happens within at the power unit.
Legacy-Support	**Enabled:** The legacy PD can be detected. **Disabled:** The legacy PD cannot be detected.
Time-Range	The time-range profile name which sets the activation time frame for a port.

Example

This example shows how to display the PoE power inline statistics.

```
Switch#show poe power-inline statistics

Interface  MPS Absent  Overload  Short  Power Denied  Invalid Signature
---------  ----------  --------  -----  ------------  -----------------
eth1/0/1       0           0       0        0               228
eth1/0/2       0           0       0        0               229
eth1/0/3       0           0       0        0               8
eth1/0/4       0           0       0        0               76
eth1/0/5       0           0       0        0               233
eth1/0/6       0           0       0        0               229
eth1/0/7       0           0       0        0               27
eth1/0/8       0           0       0        0               230
eth1/0/9       0           0       0        0               139
eth1/0/10      0           0       0        0               139
eth1/0/11      0           0       0        0               139
eth1/0/12      0           0       0        0               139
eth1/0/13      0           0       0        0               139
eth1/0/14      0           0       0        0               134
eth1/0/15      0           0       0        0               134
eth1/0/16      0           0       0        0               134
eth1/0/17      0           0       0        0               165
eth1/0/18      0           0       0        0               249
eth1/0/19      0           0       0        0               184
eth1/0/20      0           0       0        0               151
eth1/0/21      0           0       0        0               57
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

Display Parameters

MPS Absent	Increased if the PSE stops to provide power to the PI due to the PSE cannot monitor the valid MPS of PD on the PI.
Overload	If the PD is drawing too much power to exceed the maximum output power that the port can supply, the overload counter is increased.
Short	If the PD's internal circuit is shorted for some reason, this counter is increased.
Power Denied	If the PoE software system decides to disallow providing power to the attached PD, this counter is increased.
Invalid Signature	Increased if the PSE detects a PD who has an invalid PD signature.

Example

This example shows how to display the PoE power inline measurement.

```
Switch#show poe power-inline eth1/0/1-6 measurement

Interface  Voltage(V)  Current(mA)  Temperature(C)  Power(W)
---------  ----------  -----------  --------------  ---------
eth1/0/1     54.2          109          35            5.9
eth1/0/2     55            196          38            10.8
eth1/0/3     n/a           n/a          n/a           n/a
eth1/0/4     53.8          28           27            1.5
eth1/0/5     n/a           n/a          n/a           n/a
eth1/0/6     n/a           n/a          n/a           n/a

Switch#
```

This example shows how to display the PoE power inline LLDP classification.

```
Switch#show poe power-inline lldp-classification

Interface eth1/0/1
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Interface eth1/0/2
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: high
PD requested power value: 0.0W
PSE allocated power value: 0.0W

Information from PD:

none

Interface eth1/0/3
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Switch#
```

Display Parameters

Interface	The PoE interface ID.

Power type	The power type field which is in the Power via MDI TLV from PSE or PD LLDP packet.
Power source	The power source field which is in the Power via MDI TLV from PSE or PD LLDP packet.
Power priority	The power priority field which is in the Power via MDI TLV from PSE or PD LLDP packet.
PD requested power value	The PD requested power value field which is in the Power via MDI TLV from PSE or PD LLDP packet.
PSE allocated power value	The PSE allocated power value field which is in the Power via MDI TLV from PSE or PD LLDP packet.

75-10 show poe power module

This command is used to display the setting and actual values of the power modules.

show poe power module [unit *UNIT-ID***] [detail]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the stacking unit ID to be configured. This parameter is only available when the stacking mode is enabled.
detail	(Optional) Specifies to display more detailed chip parameter information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the detailed power information and PoE chip parameters for PoE modules.

Example

This example shows how to display the setting and actual values of the power modules.

```
Switch#show poe power module

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
-------------------------------------------------------------------------
1      0             370               50              Enabled    Enabled

Switch#
```

Display Parameters

Unit	The unit ID of stacking device.
Delivered	The actual amount of power delivered to the PD in watts.
Power budget	The total power can be provided by the device in watts.
Usage-Threshold	The utilization threshold to record a log.
Preempt	**Enabled:** The power management mode is policy preempt, high priority PD can preempt the provided power of lower priority PD. **Disabled:** The power management mode is first in first serviced.
Trap State	**Enabled:** The trap is sent when the PoE usage threshold exceeds the specified value. **Disabled:** The trap is not sent when the PoE usage threshold exceeds the specified value.

Example

This example shows how to display the PoE detailed parameters for unit 1.

```
Switch#show poe power module unit 1 detail

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
------------------------------------------------------------------------------
1      0             370               50              Enabled    Enabled

PoE system parameters:
Unit   Max Ports   Device ID    SW Version
----   ---------   ---------    ----------
1      24          E121         20

Switch#
```

Display Parameters

Max ports	The maximum port number of the PoE sub-system.
Device ID	The hardware version of the PoE chip.
S/W version	The firmware version of the PoE chip.

75-11 poe pd alive

This command is used to enable the PD alive check function for the PD connected to the PoE port. Use the **no** form of this command to disable the function.

poe pd alive [{ip {*IP-ADDRESS***} | interval** *INTERVAL-TIME* **| retry** *RETRY-COUNT* **| waiting-time** *WAITING-TIME* **| action {reset | notify | both}}]**

no poe pd alive [{ip | interval | retry | waiting-time | action}]

Parameters

ip	(Optional) Specifies the IPv4 address of the target PD for the system executing the ping action.

interval	(Optional) Specifies the interval for the system to issue ping requests to detect the target PD. The valid range is from 10 to 300 seconds.
retry	(Optional) Specifies the retry counts of ping requests when PD has no response. The valid range is from 0 to 5.
waiting-time	(Optional) Specifies the waiting time for PD to recover from rebooting. The valid range is from 30 to 300 seconds.
action	(Optional) Specifies the action of the system when PD does not reply the ping request. reset - Specifies to disable and then enable the PoE port state. notify - Specifies to send logs and traps to notify the administrator. both - Specifies to send log and trap first, and then reset the PoE port state.

Default

By default, this function is disabled.

The default IP address of the target PD is none.

The default interval for system to issue ping requests is 30 seconds.

The default retry counts for ping requests is 2 times.

The default waiting time for PD to recover from rebooting is 90 seconds.

The default action when PD does not reply the ping request is **both**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This function only takes effect on PoE enabled ports with power feeding.

The PD alive check function provides the solution for the PD device that stops working or has no response via the ping mechanism.

Use this command without any optional parameter to enable or disable the PD alive check function.

By default, there is no IP address of the target PD for the system to execute the ping action. The IP address of the target PD must be configured by using the **poe pd alive ip** command before executing the PD alive check.

The system needs to periodically monitor the specific PD by using the ping function. When there is no response, the system takes one of the actions configured by the **poe pd alive action** command. The interval between retry attempts can be configured by the **poe pd alive interval** command.

The system implements the retry mechanism to check the PD status. The system will reset the PoE port power feeding after the retry by using Ping without any response from a PD. The retry count can be configured by the **poe pd alive retry** command.

If the action is **reset** or **both**, the system needs to wait for PD to recover from rebooting and then executes the Ping function again. The waiting time for PD to recover from rebooting can be configured by the poe pd alive waiting-time command.

If the PoE time range function is configured on the port that also enables the PD alive check function, the time range function has higher priority, and the PD alive check function will not work When the PoE time range function is still active.

NOTE: If the PD does not support ICMP, this function cannot work normally.

NOTE: It is required to setup IP settings properly that the PD can be reached via Ping, otherwise this function cannot work as expected.

NOTE: The **reset** action can only work on the direct-connected PD. If the PD is not connected directly, the reset action may not work as expected.

NOTE: If the direct-connected PD is also a PSE, all the next level PDs connect to this PSE will be power cycling whenever the PD alive check function takes effect on the **reset** or **both** action.

Example

This example shows how to enable the PoE PD alive check function on ports 1 to 2.

```
Switch#configure terminal
Switch(config)#interface range eth1/0/1-2
Switch(config-if-range)#poe pd alive
Switch(config-if-range)#
```

This example shows how to configure the IP address of the target PD.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive ip 192.168.1.150
Switch(config-if)#
```

This example shows how to configure the interval between ping requests.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive interval 60
Switch(config-if)#
```

This example shows how to configure the retry counts of ping requests.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive retry 4
Switch(config-if)#
```

This example shows how to configure the waiting time for PD to reboot.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive waiting-time 120
Switch(config-if)#
```

This example shows how to configure the action to reset when PD does not reply.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#poe pd alive action reset
Switch(config-if)#
```

75-12 show poe pd alive

This command is used to display the PD alive check settings.

show poe pd alive [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the PD alive check settings on the specified ports. When no optional parameter is specified, information of all PoE ports will be displayed.

Example

This example shows how to display the PD alive check settings on ports 1 to 2.

```
Switch#show poe pd alive interface eth1/0/1-2

Port ID: eth1/0/1
-------------------------------------------
    PD Alive State                : Enabled
    PD IP Address                 : 0.0.0.0
    Poll Interval                 : 30
    Retry Count                   : 2
    Waiting Time                  : 90
    Action                        : both
Port ID: eth1/0/2
-------------------------------------------
    PD Alive State                : Enabled
    PD IP Address                 : 192.168.1.150
    Poll Interval                 : 60
    Retry Count                   : 4
    Waiting Time                  : 120
    Action                        : reset

Switch#
```

76. Power Saving Commands

76-1 dim led

This command is used to disable the port LED function. Use the **no** form of this command to revert to the default setting.

dim led

no dim led

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Us Use this command to turn off or turn on the port LED function. When the port LED function is disabled, LEDs used to illustrate port status are all turned off to save power.

Example

This example shows how to disable the port LED function.

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

76-2 power-saving

This command is used to enable individual power saving functions. Use the **no** form of this command to disable these functions.

power-saving {link-detection | port-shutdown | dim-led | hibernation}

no power-saving {link-detection | port-shutdown | dim-led | hibernation}

Parameters

link-detection	Specifies that power saving will be applied by link status.
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. This parameter can only be used when the stacking mode is disabled.

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 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)#
```

76-3 power-saving eee

This command is used to enable the Energy-Efficient Ethernet (EEE) function on the specified port(s). Use the **no** form of this command to disable the EEE function.

power-saving eee

no power-saving eee

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the specified port's EEE power saving function. The 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.



NOTE: EEE and ERPS are mutually exclusive functions.

Example

This example shows how to enable the EEE power saving function.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#power-saving eee
Switch(config-if)#
```

76-4 power-saving dim-led time-range

This command is used to configure the time range profile for the dim LED schedule. Use the **no** form of this command to delete the specified time range profile.

power-saving dim-led time-range *PROFILE-NAME*

no power-saving dim-led time-range *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the time range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

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 LEDs will be turned off.

Example

This example shows how to add a time-range profile for the dim LED schedule.

```
Switch#configure terminal
Switch(config)#power-saving dim-led time-range off-duty
Switch(config)#
```

76-5 power-saving hibernation time-range

This command is used to configure the time range profile for the system hibernation schedule Use the **no** form of this command to delete the specified time range profile.

power-saving hibernation time-range *PROFILE-NAME*

no power-saving hibernation time-range *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the time range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

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)#
```

76-6 power-saving shutdown time-range

This command is used to configure the time range profile for the port shutdown schedule. Use the **no** form of this command to delete the specified time range profile.

power-saving shutdown time-range *PROFILE-NAME*

no power-saving shutdown time-range *PROFILE-NAME*

Parameters

PROFILE-NAME	Specifies the name of the time range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Interface Configuration Mode.

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)#
```

76-7 show power-saving

This command is used to display the power saving configuration information.

show power-saving [link-detection] [dim-led] [port-shutdown] [hibernation] [eee]

Parameters

link-detection	(Optional) Specifies to display the link detection state.
dim-led	(Optional) Specifies to display the dim LED state.
port-shutdown	(Optional) Specifies to display the port shutdown state.
hibernation	(Optional) Specifies to display the hibernation state. This parameter can only be used when the stacking mode is disabled.
eee	(Optional) Specifies to display the EEE state.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no optional parameter is specified, all power saving configuration information will be displayed.

Example

This example shows how to display all power saving configuration information.

```
Switch#show power-saving

Link Detection Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

77. Priority-based Flow Control (PFC) Commands

77-1 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	Specifies the interfaces to be used.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
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 port 21.

```
Switch#clear priority-flow-control counters eth1/0/21 tx
Switch#
```

77-2 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 physical port interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 eth1/0/25-26 priority-flow-control

Interface PFC  Admin PFC On      Oper PFC On       Rx PFC    Tx PFC
Id        Cap. Priorities        Priorities        Frame(s)  Frame(s)
--------------------------------  ----------------  --------------------
eth1/0/25  8                     (7)               0         0
eth1/0/26  8                     (7)               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.
Admin PFC On Priorities	The CoS list that the PFC is configured to be on by the user.
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.
Rx PFC Frame(s)	The counter of received PFC frames.
Tx PFC Frame(s)	The counter of transmitted PFC frames.

78. Private VLAN Commands

78-1 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)#
```

78-2 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 VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

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)#
```

78-3 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)#
```

78-4 switchport mode private-vlan

This command is used to specify a port as a private VLAN port. The port type can be a host port or promiscuous port. Use the **no** form of this command to revert to the default setting.

switchport mode private-vlan {host | promiscuous}

no switchport mode

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.

When the port mode is changed, the settings associated with the previous mode will be lost.

Example

This example shows how to configure port 1 as a private VLAN host port and port 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)#
```

78-5 switchport private-vlan host-association

This command is used to associate the private VLAN with an isolated port, a community port, or a trunk secondary port. Use the no form of this 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

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

The port is an isolated port if the secondary VLAN specified in this command is an isolated VLAN. The port is a community port if the secondary VLAN specified in this command is a community VLAN. This command also configures the port to be an untagged member of both the primary and secondary VLANs specified.

Example

This example shows how to associate port 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)#
```

78-6 switchport private-vlan mapping

This command is used to associate the private VLAN membership with a promiscuous port or a trunk promiscuous port. Use the **no** form of this 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 VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

Use this command to associate the private VLAN membership with a promiscuous port or a trunk promiscuous port. This command also configures the port to be an untagged member of both the primary and secondary VLANs specified.

Example

This example shows how to configure port 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)#
```

78-7 show vlan private-vlan

This command is used to display private VLAN configurations.

show vlan private-vlan

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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    eth1/0/1, eth1/0/16
               1002             Community
               1003             Community
2000           2001             Isolated    eth1/0/2, eth1/0/3
2000           2002             Community   eth1/0/2, eth1/0/5
2000           2003             Community   eth1/0/4, eth1/0/13, eth1/0/15

Total Entries: 6

Switch#
```

79. Protocol Independent Commands

79-1 distance

This command is used to define an administrative distance for routing protocols including RIP and OSPF. Use the **no** form of this command to revert to the default setting.

distance *DISTANCE*

no distance

Parameters

DISTANCE	Specifies the administrative distance. The range is from 1 to 255.

Default

The default distance of a connected route is 0.

The default distance of an Open Shortest Path First (OSPF) intra-area route is 80.

The default distance of an OSPF inter-area route is 90.

The default distance of an OSPF type-1 AS external route is 110.

The default distance of an OSPF type-2 AS external route is 115.

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 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 distance of the RIP route to be 75.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distance 75
Switch(config-router)#
```

79-2 distance default

This command is used to define an administrative distance for static default route. Use the **no** form of this command to revert to the default setting.

distance default *DISTANCE*

no distance default

Parameters

DISTANCE	Specifies the administrative distance. The range is from 1 to 255.

Default

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 1 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.

Example

This example shows how to configure the static default route distance to be 150.

```
Switch#configure terminal
Switch(config)#distance default 150
Switch(config)#
```

79-3 distance static

This command is used to define an administrative distance for static routes. Use the **no** form of this command to revert to the default setting.

distance static *DISTANCE*

no distance static

Parameters

DISTANCE	Specifies the administrative distance. The range is from 1 to 255.

Default

The default distance of a static route is 60.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the distance is an integer from 1 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.

Example

This example shows how to configure the static route distance to 100.

```
Switch#configure terminal
Switch(config)#distance static 100
Switch(config)#
```

79-4 distribute-list in (OSPF)

This command is used to configure the distribute list which filters OSPF protocol route updates based on the specified access list. Use the **no** form of this command to remove the filter.

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.

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 not specified, the distribute list is applied to all interfaces.

Example

This example shows how to configure access list “East-ranch” to filter OSPF protocol route updates.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#distribute-list East-ranch in
Switch(config-router)#
```

79-5 distribute-list in (RIP)

This command is used to configure the distribute list which filters RIP protocol route updates based on the specified access list. Use the **no** form of this command to remove the filter.

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	Specifies the interface to apply the distribute list.

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.

Example

This example shows how to configure access list “branch-route” to filter RIP protocol route updates.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distribute-list branch-route in vlan1
Switch(config-router)#
```

79-6 ip route

This command is used to create a static route entry. Use the **no** form of this command to remove a static route entry.

ip route *NETWORK-PREFIX NETWORK-MASK* **{***IP-ADDRESS* **[primary | backup | weight** *NUMBER***] | null0}**

no ip route *NETWORK-PREFIX NETWORK-MASK* **{***IP-ADDRESS* **| null0}**

Parameters

NETWORK-PREFIX	Specifies the network address.
NETWORK-MASK	Specifies the network mask.
IP-ADDRESS	Specifies the IP address of the next hop that can be used to reach destination network.

primary	(Optional) Specifies the route as the primary route to the destination.
backup	(Optional) Specifies the route as the backup route to the destination.
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.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use **0.0.0.0 0.0.0.0** to specify the default route.

Floating state route is supported. This means that there could have two routes with the same destination network address but different next hop. If none of the **primary** or **backup** parameter is specified, the static route will be automatically determined to be a primary route or a backup route. Primary route is preferable, and is always be used for forwarding when it is active. When the primary route is down, the backup route will be used.

If the weight parameter is the same for multiple route paths, it is Equal-cost Multi-path (ECMP) routes .

For example:

- ip route 100.1.1.0 255.255.255.0 10.1.1.1 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.2 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.3 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.4 weight 1

If the weight parameter is different for multiple route paths, it is Weighted-cost Multi-path (WCMP) routes.

For example:

- ip route 100.1.1.0 255.255.255.0 10.1.1.1 weight 1
- ip route 100.1.1.0 255.255.255.0 10.1.1.2 weight 2
- ip route 100.1.1.0 255.255.255.0 10.1.1.3 weight 3
- ip route 100.1.1.0 255.255.255.0 10.1.1.4 weight 4

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)#
```

79-7 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***]**

no ipv6 route {default | *NETWORK-PREFIXIPREFIX-LENGTH***} [***INTERFACE-ID***]** *NEXT-HOP-ADDRESS*

Parameters

default	Specifies to add or delete a default route.
NETWORK-PREFIXIPREFIX-LENGTH	Specifies the network prefix and the prefix length of the static route.
INTERFACE-ID	(Optional) Specifies the forwarding interface for routing the packet.
NEXT-HOP-ADDRESS	Specifies the IPv6 address of the next hop to reach the destination network. If the address is a link-local address, 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 254. The lower value represents better route. If this parameter is not specified, the default administrative distance for a static route is 1.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Floating state route is supported. This means that there could have two routes with the same destination network address but different next hop. If none of the **primary** or **backup** parameter is specified, the static route will be automatically determined to be a primary route or a backup route. Primary route is preferable, and is always be used for forwarding when it is active. When the primary route is down, the backup route will be used.

Example

This example shows how to create a static route destined for the network where proxy server resides.

```
Switch#configure terminal
Switch(config)#ipv6 route 2001:0101::/32 vlan1 fe80::0000:00ff:1111:2233
Switch(config)#
```

79-8 ip route ecmp load-balance

This command is used to configure the hash load balancing algorithm to determine the next hop entry from the different paths to be destined for the same destination. Use the **no** form of this command to revert to the 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	Specifies that the load-balancing algorithm will include the lower 5 bits of the source IP address. This attribution is mutually exclusive with **crc32_lower** and **crc32_upper**. If it is set, **crc32_lower** and **crc32_upper** will be excluded.
crc32_lower	Specifies that the load-balancing algorithm will include the lower 5 bits of the CRC. This attribution is mutually exclusive with **crc32_upper** and **sip**. If it is set, **crc32_upper** and **sip** will be excluded.
crc32_upper	Specifies that the load-balancing algorithm will include the upper 5 bits of the CRC. This attribution is mutually exclusive with **crc32_lower** and **sip**. If it is set, **crc32_lower** and **sip** will be excluded.
dip	Specifies that the load-balancing algorithm will include the destination IP address.
port	Specifies that the load-balancing algorithm will include the TCP or UDP port.

Default

By default, sip is used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the hash load balancing algorithm to determine the next hop entry from the different paths to be destined for the same destination.

Example

This example shows how to configure the load-balance algorithm to be dip.

```
Switch#configure terminal
Switch(config)#ip route ecmp load-balance dip
Switch(config)#
```

79-9 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 this command to revert to the default setting.

maximum-paths *NUMBER-PATHS*

no maximum-paths

Parameters

NUMBER-PATHS	Specifies the maximum number of parallel routes.

Default

By default, the value is 1.

Command Mode

OSPF Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

There are various 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 OSPF to 4.

```
Switch#configure terminal
Switch(config)#router ospf
Switch(config-router)#maximum-paths 4
Switch(config-router)#
```

79-10 show ip protocols

This command is used to display the state of the routing process.

show ip protocols [rip | ospf]

Parameters

rip	(Optional) Specifies to display the RIP protocol overall configuration.
ospf	(Optional) Specifies to display the OSPF protocol overall configuration.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the status of the routing processes. If no parameter 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 30 seconds, next due in 9 seconds
  Invalid 180 secs, flush 120 secs
  Default redistribution metric is 0
  Redistributing: OSPF
  Default version control: send version 1, receive any version
    Interface     Send       Recv
    vlan2         1          1 2
  Maximum path: 1
  Routing for Networks:
    vlan2  (200.1.1.5/255.255.255.0)
  Routing Information Sources:
    Gateway          Last Update
  Distribute list:
    East branch (in)
    Interface   in
  Distance:100

Routing Protocol is OSPF
  Router ID 200.1.1.5
  Number of areas in this router is 2. 2 normal, 0 stub, 0 nssa
  Maximum path: 1
  Routing for Networks:
    200.1.1.5/24
  Routing Information Sources:
    Gateway
  Distribute list:
    Incoming update filter list for all interfaces is not set
  External-1 distance 110, External-2 distance 115, Inter-area distance 90, Intra-area
distance 80
Switch#
```

79-11 show ip route

This command is used to display the entry in the routing table.

show ip route [*IP-ADDRESS* **[***MASK***] | *PROTOCOL* | hardware]**

Parameters

IP-ADDRESS	(Optional) Specifies the network address of which routing information should be displayed.
MASK	(Optional) Specifies the subnet mask for the specified network.
PROTOCOL	(Optional) Specifies the following routing protocols or keywords: connected, static, RIP, and OSPF.
hardware	(Optional) Specifies to display the routes that have been written into chip.

Default

None.

Command Mode

User/Privileged EXEC 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.

Example

This example shows how to display the routing table.

```
Switch#show ip route

Code: C - connected, S - static, R - RIP, 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 not set
S    170.10.0.0/16 [60/1] via 11.0.0.2, vlan11
O    1.0.0.0/8 [80/2] via 11.0.0.1, vlan11
O    2.0.0.0/8 [80/2] via 11.0.0.1, vlan11
C    11.0.0.0/8 is directly connected, vlan11
O    12.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    13.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    17.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    18.0.0.0/8 [80/3] via 11.0.0.1, vlan11
O    30.0.0.0/8 [80/2] via 11.0.0.1, vlan11
O    40.0.0.0/8 [80/3] via 11.0.0.1, vlan11
R    105.100.0.0/24 [100/2] via 11.0.0.5, vlan11
C    107.100.0.0/16 is directly connected, vlan1
C    172.18.64.0/21 is directly connected, mgmt_ipif
R    212.254.254.0/24 [100/2] via 11.0.0.254, vlan11

Total Entries: 14

Switch#
```

79-12 show ip route summary

This command is used to display the brief information for the working routing entries.

show ip route summary

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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       3
Static          1
RIP             2
OSPF            8
Total           14
Multi-path      0

Switch#
```

79-13 show ipv6 route

This command is used to display the entry in routing table.

show ipv6 route [[*IPV6-ADDRESS* **|** *NETWORK-PREFIX/PREFIX-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 that will be used in the display.
PROTOCOL	(Optional) Specifies the routing protocol.
database	(Optional) Specifies to display all the related entries in the routing database instead of just the best route.
hardware	(Optional) Specifies to display the routes that have been written into chip.

Default

None.

Command Mode

User/Privileged EXEC 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.

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     1234::/64 [1/1] via FE80::206:28FF:FED8:FEAC, vlan11
R     2000:17::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
R     2000:18::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
C     2001:DB8:0:5::/64 [0/1] is directly connected, vlan11
O     2001:DB8:0:5::1/128 [110/10] via FE80::206:28FF:FED8:FE94, vlan11
R     2001:DB8:0:3600::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
R     2001:DB8:0:3620::/64 [71/2] via FE80::206:28FF:FED8:FE94, vlan11
R     2016:3630::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
O     2105:5000:A::/64 [110/430] via FE80::206:28FF:FED8:FE94, vlan11
C     2107:100:A::/64 [0/1] is directly connected, vlan1
O     2207:7000:AC::/64 [110/8030] via FE80::206:28FF:FED8:FE94, vlan11
O     2207:7171:ABCD::/64 [110/8040] via FE80::206:28FF:FED8:FE94, vlan11
R     6000::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11
R     7100::/64 [71/2] via FE80::206:28FF:FED8:FEAC, vlan11

Total Entries: 14 entries, 14 routes
Switch#
```

79-14 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/Privileged EXEC 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          1
RIPng           7
OSPF            4
SLAAC           0
Total           14
Switch#
```

80. Protocol Independent Multicast (PIM) Commands

80-1 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** form of this 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, 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)#
```

80-2 ip pim bsr-border

This command is used to configure the avoidance of sending and receiving BSR messages through an interface. Use the **no** form of this command to allow the message.

ip pim bsr-border

no ip pim bsr-border

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command only takes effect when the interface is PIM enabled. Use this command on the interface that border with another domain to avoid the exchange of BSR messages across two domains.

Example

This example shows how to configure VLAN 100 as a BSR border interface.

```
Switch#configure terminal
Switch(config)#interface vlan100
Switch(config-if)#ip pim bsr-border
Switch(config-if)#
```

80-3 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	(Optional) Specifies to configure the hash mask length for RP selection. The range is 0 to 32. If this parameter is not specified, the default length is 30.
PRIORITY	(Optional) 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 this parameter is not specified, the default priority is 64.
interval *SECONDS*	(Optional) Specifies the interval between originating bootstrap messages. If this parameter is 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 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)#
```

80-4 ip pim dr-priority

This command is used to configure the Designated Router (DR) priority value. Use the **no** form of this command to revert to the default setting.

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)#
```

80-5 ip pim jp-timer

This command is used to configure the Join/Prune interval value. Use the **no** form of this command to revert to 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)#
```

80-6 ip pim passive

This command is used to specify an interface running in the passive mode. Use the **no** form of this 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)#
```

80-7 ip pim query-interval

This command is used to configure the frequency of the PIM hello message. Use the **no** form of this 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 query interval to 45 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#ip pim query-interval 45
Switch(config-if)#
```

80-8 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)#
```

80-9 ip pim register-probe

This command is used to configure the register probe time. Use the **no** form of this 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)#
```

80-10 ip pim register-suppression

This command is used to configure the register suppression time. Use the **no** form of this 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)#
```

80-11 ip pim rp-address

This command is used to statically configure the RP address for multicast groups. Use the **no** form of this command to remove an RP address.

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*	(Optional) 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)#
```

80-12 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 this parameter is not 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. The default value is 60 seconds.
priority *PRIORITY*	Specifies the RP priority value. The range is from 0 to 255. The default value 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

By default, the router is not an RP candidate.

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 0.255.255.255
Switch(config-ip-acl)#exit
Switch(config)#ip pim rp-candidate vlan1 group-list PIM-Control
Switch(config)#
```

80-13 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. Use the **no** form of this command to revert to the default setting.

ip pim rp-register-kat *SECONDS*

no ip pim rp-register-kat

Parameters

SECONDS	Specifies the keep alive time. The value is 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)#
```

80-14 ip pim spt-threshold

This command is used to configure the condition to switch over to the source tree. Use the **no** form of this 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 **infinity**, 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)#
```

80-15 ip pim ssm

This command is used to configure the SSM multicast group address range. Use the **no** form of this 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 232.0.0.0/8.
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)#
```

80-16 show ip pim

This command is used to display the PIM global information.

show ip pim

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

80-17 show ip pim bsr-router

This command is used to display BSR information.

show ip pim bsr-router

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the elected BSR information and information about the locally configured candidate 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#
```

80-18 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

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.
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.

Default

None.

Command Mode

User/Privileged EXEC 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 Priority                   ID
--------------- ------------ -------- --- ---------- --------------- ----------
10.90.90.90     vlan1        DM       0   1          0.0.0.0         0

Total Entries: 1

Switch#
```

This example shows how to display interface information in detail.

```
Switch#show ip pim interface detail

vlan1
  Address             : 10.90.90.90
  PIM                 : Disabled
  Mode                : Dense
  Neighbor Count      : 0
  Generation ID       : 0
  Query Interval      : 30 seconds
  PIM Passive Mode    : Disabled


Total Entries: 1

Switch#
```

80-19 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/Privileged EXEC 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#
```

80-20 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/Privileged EXEC 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.

80-21 show ip pim rp-hash

This command is used to display the 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/Privileged EXEC 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#
```

81. Protocol Independent Multicast (PIM) IPv6 Commands

81-1 ipv6 pim

This command is used to enable IPv6 PIM on an interface. Use the **no** form of this command to disable this function.

ipv6 pim {sparse-mode | dense-mode}

no ipv6 pim [sparse-mode]

Parameters

sparse-mode	Specifies the IPv6 PIM mode as the PIM-SM.
dense-mode	Specifies the IPv6 PIM mode as PIM-DM.

Default

PIM-SM for IPv6 is disabled on all interfaces.

PIM-DM 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)#
```

81-2 ipv6 pim bsr border

This command is used to specify that the interface is a PIM domain border. Use the **no** form of this command to remove the border setting.

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)#
```

81-3 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 rendezvous point (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 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)#
```

81-4 ipv6 pim bsr candidate rp

This command is used to configure the candidate RP to send PIM RP advertisements to the 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)#
```

81-5 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 this command to revert to the default setting.

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 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, 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, the router with the highest IPv6 address will be elected as the DR.

Example

This example shows how to set 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)#
```

81-6 ipv6 pim hello-interval

This command is used to configure the frequency of PIM hello messages. Use the **no** form of this command to revert to the default setting.

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

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)#
```

81-7 ipv6 pim sr-interval

This command is used to configure the interval for state refresh messages. Use the **no** form of this command to revert to the default setting.

ipv6 pim sr-interval *SECONDS*

no ipv6 pim sr-interval

Parameters

SECONDS	Specifies the interval in seconds between state refresh messages. The range is from 4 to 100.

Default

By default, this value is 60 seconds.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the interval for state refresh messages.

Example

This example shows how to configure the interval for state refresh messages to 45 seconds.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#ipv6 pim sr-interval 45
Switch(config-if)#
```

81-8 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 revert to the default setting.

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 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)#
```

81-9 ipv6 pim passive

This command is used to specify an interface running in the passive mode. Use the **no** form of this 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)#
```

81-10 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, 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)#
```

81-11 ipv6 pim register-probe

This command is used to configure the register-probe time. Use the **no** form of this 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)#
```

81-12 ipv6 pim register-suppression

This command is used to configure the register-suppression time. Use the **no** form of this 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)#
```

81-13 ipv6 pim rp embedded

This command is used to enable embedded RP support in PIMv6. Use the **no** form of this 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)#
```

81-14 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 configure 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)#
```

81-15 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 revert to the default setting.

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)#
```

81-16 ipv6 pim ssm

This command is used to configure the SSM multicast group address range. Use the **no** form of this command to disable PIM-SSM.

ipv6 pim ssm {default | range *ACCESS-LIST***}**

no ipv6 pim ssm

Parameters

default	Specifies to use the default SSM group addresses. The default SSM group address range is FF3x::/32.
ACCESS-LIST	Specifies the standard IP access list that defines the user-specified SSM group addresses.

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.

PIM-SSM builds trees that are rooted in just one source. The SSM feature forwards datagram traffic to receivers from only those multicast sources that the receivers have explicitly joined. As a result, this optimizes bandwidth utilization and denies unwanted Internet broadcast traffic. Moreover, instead of the use of RP and shared trees, SSM uses information found on source addresses for a multicast group. This information is provided by receivers through the source addresses relayed to the last-hop devices by MLD membership reports, resulting in shortest-path trees directly to the sources.

In SSM, delivery of datagrams is based on (S, G) channels. Traffic for one (S, G) channel consists of datagrams with an IPv6 unicast source address S and the multicast group address G as the IPv6 destination address. Systems will receive this traffic by becoming members of the (S, G) channel. Signaling is not required, but receivers must subscribe or unsubscribe to (S, G) channels to receive or not receive traffic from specific sources. MLD version 2 is required for SSM to operate.

In order to achieve the full benefit of SSM, all routers in a domain should have a consistent configuration about SSM group address range.

Example

This example shows how to configure the SSM service for the IPv6 address range, ff30::/96, defined in the access list as ssm-group.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ssm-group
Switch(config-ipv6-acl)#permit any ff30::/96
Switch(config-ipv6-acl)#exit
Switch(config)#ipv6 pim ssm range ssm-group
Switch(config)#
```

81-17 ipv6 pim sg-keepalive-time

This command is used to configure the PIM6-SM multicast routing entry keep-alive timer. Use the **no** form of this command to revert to the default setting.

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)#
```

81-18 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/Privileged EXEC 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

SSM Group : Movies

Switch#
```

81-19 show ipv6 pim bsr

This command is used to display 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 display 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/Privileged EXEC 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 candidates 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.

81-20 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 BSR or static configuration.
bsr	Specifies to display ranges learned through the BSR.
embedded-rp	Specifies to display group ranges learned through the embedded RP.
static	Specifies to display ranges enabled by static configuration.

Default

None.

Command Mode

User/Privileged EXEC 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 RP.

```
Switch#show ipv6 pim group-map info-source embedded-rp

FF7E:640:2002:6666::/96
    RP: 2002:6666::6
    Info source: embedded

Switch#
```

81-21 show ipv6 pim interface

This command is used to display the configuration for PIM on interface(s).

show ipv6 pim interface [sparse-mode | dense-mode] [*INTERFACE-ID*] [detail]

Parameters

sparse-mode	(Optional) Specifies to display the PIM-SM enabled interface information.
dense-mode	(Optional) Specifies to display the PIM-DM enabled interface information.
INTERFACE-ID	(Optional) Specifies the interface to be displayed.
detail	(Optional) Specifies to display interface information in detail.

Default

None.

Command Mode

User/Privileged EXEC 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

Nbr Count: Neighbor Count

PIM6 Interface Table

Interface     Mode    Nbr    DR          Hello     J/P       BSR
                      Count  Priority    Interval  Interval  Border
------------  ------  -----  ----------  --------  --------  --------
vlan1         Sparse  0      2           30        60        disabled
    Address       : FE80::211:11FF:FE11:1111
    Global Address: 2000:1::3630
    DR            : this system
vlan2         Sparse  1      1           30        60        disabled
    Address       : FE80::211:11FF:FE11:1114
    Global Address: 2000:2::3630
    DR            : FE80::202:2FF:FE03:401

Total Entries : 2

Switch#
```

This example shows how to display 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                      : 0
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           : False
Bidirectional Capable              : False
BSR Domain Border                  : Disabled
PIM Passive Mode                   : Disabled

Total Entries : 1

Switch#
```

Display Parameters

Interface	The Interface ID that is configured to perform PIM.
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.

81-22 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/Privileged EXEC 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, s - SSM Group.

(*, 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, this timer is the remaining time before the interface to send a assert message. If the interface is an Assert Loser, 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.

81-23 show ipv6 pim neighbor

This command is used to display PIM neighbor information.

show ipv6 pim neighbor [sparse-mode | dense-mode] [detail] [*INTERFACE-ID***]**

Parameters

sparse-mode	(Optional) Specifies to display the PIM-SM neighbor information.
dense-mode	(Optional) Specifies to display the PIM-DM neighbor information.
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/Privileged EXEC 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 PIM neighbor information.

```
Switch#show ipv6 pim neighbor

Mode: B - Bidir Capable, DR - Designated Router, N - Default DR Priority,
      G - Supports Generation ID, R - State Refresh Capable
Neighbor-Address Interface Uptime/Expires              Ver   DR Pri/Mode
---------------------------------------------------------------------------
FE80::233:38FF:FE10:1700
                 vlan2     0DT01H14M18S  /0DT00H01M16S   v2    N /RG
FE80::200:FF:FE26:6667
                 vlan4     4DT18H22M00S  /0DT00H01M43S   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. **R:** The neighbor is capable of state refresh.

82. Protocol Independent Multicast (PIM) Snooping Commands

82-1 ip pim snooping

This command is used to enable the PIM snooping function. Use the no form of this command to disable this function.

ip pim snooping

no ip pim snooping

Parameters

None.

Default

By default, this function is disabled globally and on all VLAN interfaces.

Command Mode

Global Configuration Mode.

VLAN Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

For a VLAN to operate with PIM snooping, both the global state and per interface state must be enabled.

Example

This example shows how to enable the PIM snooping global state.

```
Switch#configure terminal
Switch(config)#ip pim snooping
Switch(config)#
```

This example shows how to enable PIM snooping on a VLAN 1.

```
Switch#configure terminal
Switch(config)#vlan 1
Switch(config-vlan)#ip pim snooping
Switch(config-vlan)#
```

82-2 clear ip pim snooping statistics

This command is used to clear the PIM snooping related statistics.

clear ip pim snooping statistics {all | vlan *VLAN-ID***}**

Parameters

all	Specifies to clear all PIM snooping related statistics for all VLANs.
vlan *VLAN-ID*	Specifies to clear PIM snooping related statistics for this specified VLAN.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to clear the PIM snooping related statistics.

Example

This example shows how to clear the PIM snooping related statistics.

```
Switch#clear ip pim snooping statistics all
Switch#
```

82-3 show ip pim snooping

This command is used to display PIM snooping information on the Switch.

show ip pim snooping [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display PIM snooping information on the Switch.

Example

This example shows how to display global PIM snooping information on the Switch.

```
Switch#show ip pim snooping

PIM snooping global state       : Enabled
Number of user enabled VLANs    : 2
User enabled VLANs: 1, 2

Switch#
```

This example shows how to display PIM snooping information for a specific VLAN.

```
Switch#show ip pim snooping vlan 1

2 neighbors, 10 mroutes, DR is 36.90.90.100
Learned neighbor on ports:
  1/0/23, Local

Switch#
```

82-4 show ip pim snooping neighbor

This command is used to display PIM snooping neighbor information on the Switch.

show ip pim snooping neighbor [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display PIM snooping neighbor information on the Switch.

Example

This example shows how to display PIM snooping neighbor information on the Switch.

```
Switch#show ip pim snooping neighbor

Mode: DR - Designated Router, L - LAN Prune Delay , T - Tracking

VLAN  Neighbor        Port         Uptime/Expires                Option Flags
1     36.90.90.90     1/0/23        0DT00H09M30S/0DT00H01M45S
1     36.90.90.100    Local         0DT00H09M28S/0DT00H01M18S      DR

Total Entries: 2

Switch#
```

82-5 show ip pim snooping mroute

This command is used to display PIM snooping multicast routing information on the Switch.

show ip pim snooping mroute [vlan *VLAN-ID* **| group** *GROUP-ADDRESS***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.
group *GROUP-ADDRESS*	(Optional) Specifies the group address to display the mroute for the group.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display PIM snooping multicast routing information on the Switch.

Example

This example shows how to display PIM snooping multicast routing information on the Switch.

```
Switch#show ip pim snooping mroute

Timers: PPT - Prune Pending Timer, ET - Expiry Timer

VLAN 1, (*, 226.1.1.1)
  Uptime/Expire: 0DT00H07M21S/0DT00H03M08S
  Downstream ports: 1/0/23
  Outgoing ports: 1/0/23, Local
    Port 1/0/23, JPState:Join, Exp:0DT00H03M08S
        Upstream neighbor: 36.90.90.100 learned on port Local
            PPT/ET: -/0DT00H03M08S

VLAN 1, (*, 226.1.1.2)
  Uptime/Expire: 0DT00H07M21S/0DT00H03M08S
  Downstream ports: 1/0/23
  Outgoing ports: 1/0/23, Local
    Port 1/0/23, JPState:Join, Exp:0DT00H03M08S
        Upstream neighbor: 36.90.90.100 learned on port Local
            PPT/ET: -/0DT00H03M08S

VLAN 1, (1.3.3.5, 226.1.1.2, rpt)
  Uptime/Expire: 0DT00H07M18S/0DT00H03M08S
  Downstream ports: 1/0/23
  Outgoing ports: 1/0/23, Local
    Port 1/0/23, JPState:Pruned, Exp:0DT00H03M08S
        Upstream neighbor: 36.90.90.100 learned on port Local
            PPT/ET: -/0DT00H03M08S

Total Entries: 3

Switch#
```

82-6 show ip pim snooping statistics

This command is used to display PIM snooping statistics information on the Switch.

show ip pim snooping statistics [vlan *VLAN-ID***]**

Parameters

vlan *VLAN-ID*	(Optional) Specifies the VLAN to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display PIM snooping statistics information on the Switch.

Example

This example shows how to display PIM snooping statistics information on the Switch.

```
Switch#show ip pim snooping statistics

VLAN ID: 1
Received PIMv2 hello: 41
Received PIMv2 join/prune: 18
Received PIM error: 0
Received PIMv1 messages in total: 0
Received PIMv2 messages in total: 69

VLAN ID: 2
Received PIMv2 hello: 0
Received PIMv2 join/prune: 0
Received PIM error: 0
Received PIMv1 messages in total: 0
Received PIMv2 messages in total: 0

Total Entries: 2

Switch#
```

83. Quality of Service (QoS) Commands

83-1 class

This command is used to specify the name of the class map to be associated with a traffic policy and then enter into policy map class configuration mode. Use the **no** form of this command to remove the policy definition for the specified class.

class *NAME*

no class *NAME*

class class-default

Parameters

NAME	Specifies the name of the class map to be associated with a traffic policy.

Default

None.

Command Mode

Policy-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to the Policy-map Configuration Mode. All the traffic that does not match the proceeding defined class will be classified as class-default. If the specified name of class map does not exist, no traffic is classified to the class.

Example

This example shows how to define a policy map, policy1, which defines policies for the class “class-dscp-red”. The packets that match DSCP 10, 12, or 14 will all be marked as DSCP 10 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)#
```

83-2 class-map

This command is used to create or modify a class-map that defines the criteria for packet matching, or enter the Class-map Configuration mode. Use the **no** form of this command to remove an existing class map from the Switch.

class-map [match-all | match-any] *NAME*

no class-map *NAME*

Parameters

match-all	(Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical AND. If neither **match-all** nor **match-any** is specified, **match-any** is implied.
match-any	(Optional) Specifies how to evaluate multiple match criteria. Multiple match statements in the class map will be evaluated based on the logical OR. If neither **match-all** nor **match-any** is specified, **match-any** is implied.
NAME	Specifies the name of the class map with a maximum of 32 characters.

Default

By default, only class-default exists.

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)#
```

83-3 match

This command is used to define the match criteria for a class-map. Use the **no** form of this command to remove the match criteria.

match {access-group name *ACCESS-LIST-NAME* **| cos [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 [inner] *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. **inner** - (Optional) 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. **ip** - (Optional) Specifies that the match is for IPv4 packets only. If this parameter is not specified, the match is for both IPv4 and IPv6 packets.
[ip] precedence *IP-PRECEDENCE-LIST*	Specifies IP precedence values to be matched. Enter one or more precedence values separated by commas or hyphen for a range list. The valid range is from 0 to 7. **ip** - (Optional) Specifies that the match is for IPv4 packets only. If this parameter is 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 [inner] *VLAN-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 **match access-group** command specifies an access list that will be matched. The packets that are permitted by the access list will be included in the class. The deny rule in the access list will be ignored. When the access group is applied using the **expert access-group**, **ip access-group**, **ipv6 access-group**, or **mac access-group** commands, and when the packet is matched in the ACL and QoS rules, the action of the class map will take effect.

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 to create classes called voice and video-n-data 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 port 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)#policy-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 eth1/0/1
Switch(config-if)#service-policy input cos-based-treatment
Switch(config-if)#
```

83-4 mls qos aggregate-policer

This command is used to define a named aggregate policer for use in policy maps. Use the **no** form of this command to delete a named aggregate policer. 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	(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.
conform-action	(Optional) Specifies the action to take on green color packets. If this parameter 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 this parameter 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 this parameter is not specified, the default action is the same as **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 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)#
```

83-5 mls qos cos

This command is used to configure the default Class of Service (CoS) value of a port. Use the **no** form of this command to revert to the default setting.

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.

By default, **override** is not specified.

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 to configure the default CoS value to 3 on port 1.

```
Switch#configure terminal
Switch(config)#interface  eth1/0/1
Switch(config-if)#mls qos cos 3
Switch(config-if)#
```

83-6 mls qos dscp-mutation

This command is used to attach an ingress Differentiated Services Code Point (DSCP) mutation map to the interface. Use the no form of this command to remove the ingress DSCP mutation map association from the interface.

mls qos dscp-mutation *DSCP-MUTATION-TABLE-NAME*

no mls qos dscp-mutation

Parameters

DSCP-MUTATION-TABLE-NAME	Specifies the name of the DSCP mutation table. The string of the name is up to 32 characters and no space is allowed.

Default

None.

Command Mode

Interface Configuration Mode.

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 attach the ingress-DSCP mutation map named “mutemap1” to port 1.

```
Switch#configure terminal
Switch(config)#mls qos map dscp-mutation mutemap1 30 to 8
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos dscp-mutation mutemap1
Switch(config-if)#
```

83-7 mls qos map cos-color

This command is used to define the CoS to color map for mapping a packet’s initial color. Use the **no** form of this command to revert to the default setting.

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. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.
green	Specifies to be mapped to green.
yellow	Specifies to be mapped to yellow.
red	Specifies to be mapped to red.

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 this command 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 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos map cos-color 1-7 to red
Switch(config-if)#
```

83-8 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. Use the **no** form of this command to revert to the default setting.

mls qos map dscp-color *DSCP-LIST* **to {green | yellow | red}**

no mls qos map dscp-color *DSCP-LIST*

Parameters

DSCP-LIST	Specifies the list of DSCP code point to be mapped to a color. The range is from 0 to 63. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.
green	Specifies to be mapped to green.
yellow	Specifies to be mapped to yellow.
red	Specifies to be mapped to red.

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 on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos map dscp-color 61-63 to yellow
Switch(config-if)#
```

83-9 mls qos map dscp-cos

This command is used to define a DSCP-to-CoS map. Use the **no** form of this command to revert to the default setting.

mls qos map dscp-cos *DSCP-LIST* **to** *COS-VALUE*

no mls qos map dscp-cos *DSCP-LIST*

Parameters

dscp-cos *DSCP-LIST* **to** *COST-VALUE*	Specifies the list of DSCP code points to be mapped to a CoS value. The range is from 0 to 63. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.
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 on port 6.

```
Switch#configure terminal
Switch(config)#interface eth1/0/6
Switch(config-if)#mls qos map dscp-cos 12,16,18 to 1
Switch(config-if)#
```

83-10 mls qos map dscp-mutation

This command is used to define a named DSCP mutation map. Use the **no** form of this command to remove the mutation map.

mls qos map dscp-mutation *MAP-NAME INPUT-DSCP-LIST* **to** *OUTPUT-DSCP*

no mls qos map dscp-mutation *MAP-NAME*

Parameters

MAP-NAME	Specifies the name of the DSCP mutation map in a string length up to 32 characters (no space is allowed).
INPUT-DSCP-LIST	Specifies the list of DSCP code point to be mutated to another DSCP value. The range is from 0 to 63. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.
OUTPUT-DSCP	Specifies the mutated DSCP value. The value is 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)#
```

83-11 mls qos scheduler

This command is used to configure the scheduling mechanism. Use the **no** form of this command to revert to the default setting.

mls qos scheduler {sp | rr | wrr | wdrr}

no mls qos scheduler

Parameters

sp	Specifies that all queues are in Strict Priority (SP) scheduling.
rr	Specifies that all queues are in Round-Robin (RR) scheduling.

wrr	Specifies the queues in the frame count Weighted Round-Robin (WRR) scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode.
wdrr	Specifies the queues of all ports in the frame length (quantum) Weighted Deficit Round-Robin (WDRR) scheduling. If the weight of a queue be configured to zero, the queue is in the SP scheduling mode.

Default

The default queue scheduling algorithm is WRR.

Command Mode

Interface Configuration Mode.

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 eth1/0/1
Switch(config-if)#mls qos scheduler sp
Switch(config-if)#
```

83-12 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 this command to revert to the default setting.

mls qos trust {cos | dscp}

no mls qos trust

Parameters

cos	Specifies that the CoS bits of the arriving packets are trusted for subsequent QoS operations.
dscp	Specifies that the ToS/DSCP bits, if available in the arriving packets, are trusted for subsequent operations. For non-IP packet, Layer 2 CoS information will be trusted for traffic classification.

Default

By default, CoS is trusted.

Command Mode

Interface Configuration Mode.

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, 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, 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, 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 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)#
```

83-13 police

This command is used to configure traffic policing to use the single rate. Use the **no** form of this command to remove traffic policing.

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, 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. 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 on port 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 eth1/0/1
Switch(config-if)#service-policy input police-setting
Switch(config-if)#
```

83-14 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** form of this 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)#
```

83-15 police cir

This command is used to configure traffic policing for two rates, the CIR and the PIR. Use the **no** form of this 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 this parameter 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 this parameter 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 this parameter is not specified, the default action is the same as **exceed-action**.
ACTION	(Optional) 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, **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 to configure two-rate traffic policing 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 port 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)#
```

83-16 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. Use the **no** form of this command to delete a policy map.

policy-map *NAME*

no policy-map *NAME*

Parameters

NAME	Specifies the name of the policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None.

Command Mode

Global Configuration Mode.

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 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 0
Switch(config-pmap-c)#
```

83-17 priority-queue cos-map

This command is used to define a CoS to queue map. Use the **no** form of this command to revert to the default setting.

priority-queue cos-map *QUEUE-ID COS1* **[***COS2* **[***COS3* **[***COS4* **[***COS5* **[***COS6* **[***COS7* **[***COS8***]]]]]]]**

no priority-queue cos-map

Parameters

QUEUE-ID	Specifies the queue ID the CoS will be mapped.
COS1	Specifies the mapping CoS value. Valid values are from 0 to 7.

COS2…COS8	(Optional) Specifies the mapping CoS value. Valid values are from 0 to 7.

Default

The default priority (CoS) to queue mapping is: 0 to 2, 1 to 0, 2 to 1, 3 to 3, 4 to 4, 5 to 5, 6 to 6, 7 to 7.

Command Mode

Global Configuration Mode.

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)#
```

83-18 queue rate-limit

This command is used to specify or modify the bandwidth allocated for a queue. Use the **no** form of this command to remove the bandwidth allocated for a queue.

queue *QUEUE-ID* **rate-limit {***MIN-BANDWIDTH-KBPS* **| percent** *MIN-PERCENTAGE***} {***MAX-BANDWIDTH-KBPS* **| percent** *MAX-PERCENTAGE***}**

no queue *QUEUE-ID* **rate-limit**

Parameters

QUEUE-ID	Specifies the queue ID to set minimal guaranteed and maximum bandwidth.
MIN-BANDWIDTH-KBPS	Specifies the minimal guaranteed bandwidth in kilobits per second allocated to a specified queue.
MAX-BANDWIDTH-KBPS	Specifies the maximum bandwidth in kilobits per second for a specified queue.
MIN-PERCENTAGE	Specifies to set the minimal bandwidth by percentage. The valid range is from 1 to 100.
MAX-PERCENTAGE	Specifies to set the maximum bandwidth by percentage. The valid range is from 1 to 100.

Default

None.

Command Mode

Interface Configuration Mode.

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 port 1 to 100Kbps and 2000Kbps respectively. Set the minimum guaranteed bandwidth and maximum bandwidth of queue 2 to 10% and 50% respectively.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#queue 1 rate-limit 100 2000
Switch(config-if)#queue 2 rate-limit percent 10 percent 50
Switch(config-if)#
```

83-19 rate-limit {input | output}

This command is used to set the received or transmitted bandwidth limit values for an interface. Use the **no** form of this command to disable the bandwidth limit.

rate-limit {input | output} {*NUMBER-KBPS* **| percent** *PERCENTAGE***} [***BURST-SIZE***]**

no rate-limit {input | output}

Parameters

input	Specifies the bandwidth limit for ingress packets.
output	Specifies the bandwidth limit for egress packets.
NUMBER-KBPS	Specifies the number of kilobits per second as the maximum bandwidth limit.
PERCENTAGE	Specifies to set the limited rate by percentage. The valid range is 1 to 100.
BURST-SIZE	(Optional) Specifies the limit for burst traffic in Kbyte.

Default

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 to configure the maximum bandwidth limits on port 5. The ingress bandwidth is limited to 2000Kbps and 4096K bytes for burst traffic.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#rate-limit input 2000 4096
Switch(config-if)#
```

83-20 service-policy

This command is used to attach a policy map to the input or output type on an interface. Use the **no** form of this command to remove a service policy from an input interface.

service-policy {input | output} *NAME*

no service-policy {input | output}

Parameters

input	Specifies to apply the policy map for ingress flow on the interface.
output	Specifies to apply the policy map for egress flow on the interface.
NAME	Specifies the name of a service policy map. The name can be a maximum of 32 alphanumeric characters.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

Use this command to attach at most one policy map for each type (input or output) on an interface. This policy is attached to the interface for aggregate and controls the number or rate of packets. A packet arriving at a port will be treated based on the service policy attached to the interface.

Example

This example shows how to define two policy maps: (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 ports 1 and 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 800 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#exit
Switch(config-pmap)#class silver
Switch(config-pmap-c)#police 2000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#exit
Switch(config-pmap)#class bronze
Switch(config-pmap-c)#police 8000 2000 exceed-action set-dscp-transmit 0
Switch(config-pmap-c)#exit
Switch(config-pmap)#exit
Switch(config)#interface eth1/0/1
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#service-policy input cust1-classes
Switch(config-if)#
```

83-21 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. Use the **no** form of this command to remove the set.

set {[ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

no set {[ip] precedence *PRECEDENCE* **| [ip] dscp** *DSCP* **| cos** *COS* **| cos-queue** *COS-QUEUE***}**

Parameters

[ip] precedence *PRECEDENCE*	Specifies a new precedence for the packet. The valid range is from 0 to 7. **ip** - (Optional) Specifies to mark that IPv4 precedence. If this parameter is 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.
[ip] dscp *DSCP*	Specifies a new DSCP for the packet. The valid range is from 0 to 63. **ip** - (Optional) Specifies to mark that IPv4 DSCP. If this parameter is not specified, both IPv4 and IPv6 DSCP will be marked. Setting DSCP will not affect the CoS queue selection.

cos *COS*	Specifies the new CoS value to the packet. The range is from 0 to 7. Setting the CoS will affect the CoS queue selection while the policy map is applied on the ingress interface.
cos-queue *COS-QUEUE*	Specifies the new CoS queue value to the packets. This will overwrite 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 to configure the policy map “policy1” with the policy for the class1 class. The packets that are included in the class1 class will be set to a DSCP of 10 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)#
```

83-22 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 32 alphanumeric characters.

Default

None.

Command Mode

User/Privileged EXEC 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 to define two class maps. Packets that match the access list “acl_home_user” belong to the class “c3”, IP packets belong to the class “c2”.

```
Switch#show class-map

Class Map match-any class-default
   Match any

 Class Map match-all c2
   Match protocol ip

Class Map match-all c3
   Match access-group acl_home_user

Switch#
```

83-23 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/Privileged EXEC 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#
```

83-24 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-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
cos	Specifies to display the port default CoS.
scheduler	Specifies to display the transmit queue scheduling settings.
trust	Specifies to display the port trust State.
rate-limit	Specifies to display the bandwidth limitation configured for the port.
queue-rate-limit	Specifies to display the bandwidth allocation configured for the queue.
dscp-mutation	Specifies to display the DSCP mutation map attached to the interface.
map dscp-color	Specifies to display the DSCP to color map.
map cos-color	Specifies to display the CoS to color map.
map dscp-cos	Specifies to display the mapping of DSCP to CoS

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

When use the rate-limit or queue-rate-limit parameter to display, the information is displayed by percentage and actual rate if the port link is up, and the information is displayed by percentage if the port link is down.

Example

This example shows how to display the default CoS for ports 2 to 5.

```
Switch#show mls qos interface eth1/0/2-5 cos

 Interface     CoS   Override
 ------------  ----  ---------
 eth1/0/2      3     Yes
 eth1/0/3      4     No
 eth1/0/4      4     No
 eth1/0/5      3     No

Switch#
```

This example shows how to display the port trust state for ports 2 to 5.

```
Switch#show mls qos interface eth1/0/2-5 trust

 Interface     Trust State
 ------------  ------------
 eth1/0/2      trust DSCP
 eth1/0/3      trust CoS
 eth1/0/4      trust DSCP
 eth1/0/5      trust CoS

Switch#
```

This example shows how to display the scheduling configuration for ports 1 to 2.

```
Switch#show mls qos interface eth1/0/1-2 scheduler

 Interface     Scheduler Method
 ------------  -----------------
 eth1/0/1      sp
 eth1/0/2      wrr

Switch#
```

This example shows how to display the DSCP mutation maps attached to ports 1 to 2.

```
Switch#show mls qos interface eth1/0/1-2 dscp-mutation

 Interface     DSCP Mutation Map
 ------------  --------------------
 eth1/0/1      Mutate Map 1
 eth1/0/2      Mutate Map 2

Switch#
```

This example shows how to display the bandwidth allocation for ports 1 to 4.

```
Switch#show mls qos interface eth1/0/1-4 rate-limit

 Interface Rx Rate             TX Rate             Rx Burst       Tx Burst
 --------- ------------------- ------------------- -------------- -------------
 eth1/0/1  1000 kbps           No Limit            64 kbyte       No Limit
 eth1/0/2  No Limit            2000 kbps           No Limit       2000 kbyte
 eth1/0/3  10%(100000 kbps)    20%(200000 kbps)    64 kbyte       64 kbyte
 eth1/0/4  2%                  2000 kbps           64 kbyte       64 kbyte

Switch#
```

This example shows how to display the CoS bandwidth allocation for ports 1 to 2.

```
Switch#show mls qos interface eth1/0/1-2 queue-rate-limit


eth1/0/1
 QID   Min Bandwidth        Max Bandwidth
 ----  -------------------  -------------------
 0     No Limit             No Limit
 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 ports 1 to 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 0-63 are mapped to green

Switch#
```

This example shows how to display the CoS to color map for ports 3 to 4.

```
Switch#show mls qos interface eth1/0/3-4 map cos-color


eth1/0/3
  CoS 0-2,5,7 are mapped to green
  CoS 3-4 are mapped to yellow
  CoS 6 are mapped to red

eth1/0/4
  CoS 0-6 are mapped to green
  CoS 7 are mapped to yellow

Switch#
```

This example shows how to display the DSCP to CoS map for port 1.

```
Switch#show mls qos interface eth1/0/1 map dscp-cos

eth1/0/1
        0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 00 00 00 00 00 00 00 01 01
   10  01 01 01 01 01 01 02 02 02 02
   20  02 02 02 02 03 03 03 03 03 03
   30  03 03 04 04 04 04 04 04 04 04
   40  05 05 05 05 05 05 05 05 06 06
   50  06 06 06 06 06 06 07 07 07 07
   60  07 07 07 07


Switch#
```

83-25 show mls qos map dscp-mutation

This command is used to display the QoS DSCP mutation map configuration.

show mls qos maps dscp-mutation [*MAP-NAME***]**

Parameters

MAP-NAME	(Optional) Specifies the name of the DSCP mutation map to be displayed.

Default

None.

Command Mode

User/Privileged EXEC 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: mutation
Attaching interface:
   eth1/0/2-1/0/3,1/0/8-1/0/10

       0  1  2  3  4  5  6  7  8  9
     ---------------------------------
   00  00 10 02 10 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#
```

83-26 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 separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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   QID
   ---   ---
    0     2
    1     0
    2     1
    3     3
    4     4
    5     5
    6     6
    7     7


Switch#
```

This example shows how to display the weight configuration for the different scheduler on port 3.

```
Switch#show mls qos queueing interface eth1/0/3

Interface: eth1/0/3
 wrr bandwidth weights:
   QID  Weights
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      0
 wdrr bandwidth weights:
   QID  Quantum
   ---  -------
    0      1
    1      1
    2      1
    3      1
    4      1
    5      1
    6      1
    7      1

Switch#
```

83-27 show policy-map

This command is used to display the policy map configuration.

show policy-map [*POLICY-NAME* **| interface** *INTERFACE-ID***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the policy map. If this parameter is not specified, all policy maps will be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the physical port interfaces to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the class policy configured for the policy map.

Example

This example shows how to configure two-rate traffic policing in the policy map "policy1" for the class "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)#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 eth1/0/1
Router(config-if)#service-policy output policy1
Router(config-if)#
```

This example shows how to display the policy map "policy1".

```
Switch#show policy-map policy1

 Policy Map policy1
  Class Map 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 on port 1.

```
Switch#show policy-map interface eth1/0/1

 Policy Map: policy1 : output
  Class Map police
   police cir 500 bc 10 pir 1000 be 10 conform-action transmit exceed-action set-dscp-transmit
2 violate-action drop

Switch#
```

83-28 wdrr-queue bandwidth

This command is used to set the queue quantum in the WDRR scheduling mode. Use the **no** form of this command to revert to the default setting.

wdrr-queue bandwidth *QUANTUM1…QUANTUM8*

no wdrr-queue bandwidth

Parameters

QUANTUM1 …QUANTUM8	Specifies the quantum (frame length count) value of every queue for weighted round-robin scheduling.

Default

By default, each quantum value is 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the scheduling mode is in the WDRR mode. Use the **mls qos scheduler wdrr** command to change the scheduling mode to the WDRR mode.

Example

This example shows how to configure the queue quantum of the WDRR scheduling mode, queue quantum of queue 0, queue 1, queue 2, queue 3, queue 4, queue 5, queue 6, queue 7 are 1, 2, 3, 4, 5, 6, 7, 8 respectively on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler wdrr
Switch(config-if)#wdrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

83-29 wrr-queue bandwidth

This command is used to set the queue weight in the WRR scheduling mode. Use the **no** form of this command to revert to the default setting.

wrr-queue bandwidth *WEIGHT1…WEIGHT8*

no wrr-queue bandwidth

Parameters

WEIGHT1 …WEIGHT8	Specifies the weight value (frame count) for each of the eight weight queues used in WRR scheduling. The weight value range is from 0 to 127.

Default

By default, the weight value for *WEIGHT1* to *WIGHT7* is 1.

By default, the weight value for *WEIGHT8* is 0.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command takes effect when the scheduling mode is in the WDRR mode. Use the **mls qos scheduler wdrr** command to change the scheduling mode to the WDRR mode. To meet the behavior requirements of Expedited Forwarding (EF), the highest queue is always selected by the Per-hop Behavior (PHB) EF and the schedule mode of this queue should be strict priority scheduling. So, the weight of the last queue should be zero while the Differentiate Service is supported.

Example

This example shows how to configure the queue weight of the WRR scheduling mode, queue weight of queue 0, queue 1, queue 2, queue 3, queue 4, queue 5, queue 6, queue 7 are 1, 2, 3, 4, 5, 6, 7, 8 respectively on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#mls qos scheduler wrr
Switch(config-if)#wrr-queue bandwidth 1 2 3 4 5 6 7 8
Switch(config-if)#
```

84. QoS Amendment Data Center Bridge (DCB) Commands

84-1 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)#
```

84-2 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:** Defines the class of traffic in a type network QoS class map.
- **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)#
```

84-3 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 this command to disable 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 on port 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-nq)#
```

Step 3: Apply the type network QoS policy map, “my_policy_map”, created in step 2, on port 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)#
```

84-4 policy-map type network-qos

This command is used to enter the Policy-map Configuration Mode to 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 enter the Policy-map Configuration Mode.

```
Switch#configure terminal
Switch(config)#policy-map type network-qos my_policy_map
Switch(config-pmap-nq)#
```

84-5 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 32 alphanumeric 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 my_policy_map to a physical ingress interface.

```
Switch#configure terminal
Switch(config)#interface eth1/0/26
Switch(config-if)#service-policy type network-qos input my_policy_map
Switch(config-if)#
```

84-6 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 32 alphanumeric characters.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

84-7 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/Privileged EXEC 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 display the policy maps configuration, if any, that has been attached to the specified interface.

```
Switch#show policy-map interface eth1/0/1

Policy Map: policy1(network-qos) : input
Class Map my_class_map_2

pause
Policy Map: policy2 : input
  Class Map police
police cir 500000 bc 10000 pir 1000000 be 10000 exceed-action set-dscp-transmit 2 violate-action drop

Switch#
```

84-8 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 this parameter is not specified, all type network QoS policy maps will be displayed.
interface *INTERFACE-ID*	(Optional) Specifies the module and port number.

Default

None.

Command Mode

User/Privileged EXEC 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 Map my_class_map
   pause

Switch#
```

85. Remote Network MONitoring (RMON) Commands

85-1 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 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

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

The RMON statistics group entry number is dynamic. Only the interface that is enabled for RMON statistics will have a corresponding entry in the table.

Example

This example shows how to configure an RMON statistics entry with an index of 65 and the owner name “guest” on port 2.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#rmon collection stats 65 owner guest
Switch(config-if)#
```

85-2 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 this parameter is 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

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

The RMON history group entry number is dynamic. Only the interface that is enabled for RMON history statistics gathering will have a corresponding entry in the table. The configured interface becomes the data source for the created entry.

Example

This example shows how to enable the RMON MIB history statistics group on port 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#rmon collection history 101 owner it@domain.com interval 2000
Switch(config-if)#
```

85-3 rmon alarm

This command is used to configure an alarm entry to monitor an interface. . Use the **no** form of this command to remove an alarm entry.

rmon alarm *INDEX VARIABLE INTERVAL* **{delta | absolute} rising-threshold** *VALUE* **[***RISING-EVENT-NUMBER***] falling-threshold** *VALUE* **[***FALLING-EVENT-NUMBER***] [owner** *STRING***]**

no rmon alarm *INDEX*

Parameters

INDEX	Specifies the alarm index. The range is from 1 to 65535.
VARIABLE	Specifies the object identifier of the variable to be sampled.
INTERVAL	Specifies the interval in seconds for the sampling of the variable and checking against the threshold. The valid range is from 1 to 2147483647.
delta	Specifies that the delta of two consecutive sampled values is monitored.

absolute	Specifies that the absolute sampled value is monitored.
rising-threshold *VALUE*	Specifies the rising threshold. The valid range is from 0 to 2147483647.
RISING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the ringing threshold crossing event. The valid range is from 1 to 65535. If this parameter is 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 this parameter is not specified, no action is taken while crossing the falling threshold.
owner *STRING*	(Optional) 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)#
```

85-4 rmon event

This command is used to configure an event entry. Use the **no** form of this command to remove an event entry.

rmon event *INDEX* **[log] [[trap** *COMMUNITY***] [owner** *NAME***] [description** *TEXT***]**

no rmon event *INDEX*

Parameters

INDEX	Specifies the index of the alarm entry. The valid range is from 1 to 65535.
log	(Optional) Specifies to generate log message for the notification.
trap *COMMUNITY*	(Optional) Specifies to generate SNMP trap messages for the notification. The maximum length is 127.
owner *NAME*	(Optional) Specifies the owner string. The maximum length is 127.
description *STRING*	(Optional) Specifies a description for the RMON event entry. Enter a text string with a maximum length of 127 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the **log** parameter is specified but not the **trap** parameter, the created entry will cause a log entry to be generated on an event occurrence. If the **trap** parameter is specified but not the **log** parameter, the created entry will cause an SNMP notification to be generated on an event occurrence.

If both **log** and **trap** are specified, the created entry will cause both the log entry and the SNMP notification to be generated on event occurrence.

Example

This example shows how to configure an event with an index of 13 to generate a log on the occurrence of the event.

```
Switch#configure terminal
Switch(config)#rmon event 13 log owner it@domain.com description ifInNUcastPkts is too much
Switch(config)#
```

85-5 show rmon alarm

This command is used to display the alarm configuration.

show rmon alarm

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the RMON alarm table.

Example

This example shows how to display the RMON alarm table.

```
Switch#show rmon alarm

Alarm index 23, owned by IT
  Monitors OID: 1.3.6.1.2.1.2.2.1.10.1
  every 120 second(s)
  Taking delta samples, last value was 2500
  Rising threshold is 2000, assigned to event 12
  Falling threshold is 1100, assigned to event 12
  On startup enable rising or falling alarm

Switch#
```

85-6 show rmon events

This command is used to display the RMON event table.

show rmon events

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command displays the RMON event table.

Example

This example shows how to display the RMON event table.

```
Switch#show rmon events

Event 1, owned by manager1
  Description is Errors
  Event trigger action: log & trap sent to community manager
  Last triggered time: 13:12:15, 2013-03-02

Event 2, owned by manager2
  Description is Errors
  Event trigger action: log & trap
  Last triggered time:

Switch#
```

85-7 show rmon history

This command is used to display RMON history statistics information.

show rmon history

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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 eth1/0/2
  Interval: 30 seconds
  Requested buckets: 50, Granted buckets: 50
  Sample #1
    Received octets: 303595962, Received packets: 357568
    Broadcast packets: 3289, Multicast  packets: 7287
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Sample #2
    Received octets: 303596354, Received packets: 357898
    Broadcast packets: 3329, Multicast  packets: 7337
    Estimated utilization: 19
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0

Switch#
```

85-8 show rmon statistics

This command is used to display RMON Ethernet statistics.

show rmon statistics

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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  eth1/0/3
  Received Octets : 234000, Received packets : 9706
  Broadcast packets: 2266, Multicast packets: 192
    Undersized packets: 213, Oversized  packets: 24
    Fragments: 2, Jabbers: 1
    CRC alignment errors: 0, Collisions: 0
  Drop events : 0
  Packets in 64 octets: 256, Packets in 65-127 octets : 236
  Packets in 128-255 octets : 129, Packets in 256-511 octets : 10
  Packets in 512-1023 octets : 38, Packets in 1024-1518 octets : 2200

Switch#
```

85-9 snmp-server enable traps rmon

This command is used to enable the sending of RMON traps. Use the **no** form of this command to disable the sending of RMON traps.

snmp-server enable traps rmon [rising-alarm | falling-alarm]

no snmp-server enable traps rmon [rising-alarm | falling-alarm]

Parameters

rising-alarm	(Optional) Specifies to configure the rising alarm trap state.
falling-alarm	(Optional) Specifies to configure the falling alarm trap state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of RMON traps.

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)#
```

86. Reset Button Commands

86-1 reset-button reboot

This command is used to enable the reboot state of the reset button on the Switch. Use the **no** form of this command to disable the function.

reset-button reboot enable

no reset-button reboot

Parameters

None.

Default

By default, this function is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the reboot state of the reset button on the Switch. When enabled, pressing the reset button on the Switch within 5 seconds will reboot the Switch.

Example

This example shows how to disable the reboot state of the reset button on the Switch.

```
Switch#configure terminal
Switch(config)#no reset-button reboot
Switch(config)#
```

86-2 reset-button ztp

This command is used to enable the Zero Touch Provisioning (ZTP) state of the reset button on the Switch. Use the **no** form of this command to disable the function.

reset-button ztp enable

no reset-button ztp

Parameters

None.

Default

By default, this function is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the ZTP state of the reset button on the Switch. When enabled, pressing the reset button on the Switch between 5 and 10 seconds will initiate ZTP. The DUT starts the ZTP function, obtains , and applies the image and configuration to the VLAN 1 interface using DHCP and TFTP. At the same time, all the LEDs blink green to indicate that the ZTP process is active.

The downloaded image and configuration is then used on the Switch after it rebooted. If the download failed, all the LEDs light solid amber. When the download failed, the image and configuration is left unchanged and the Switch does not reboot. Press the reset button to return the LEDs to their normal state.

Example

This example shows how to disable the ZTP state of the reset button on the Switch.

```
Switch#configure terminal
Switch(config)#no reset-button ztp
Switch(config)#
```

86-3 reset-button factory

This command is used to enable the factory reset state of the reset button on the Switch. Use the **no** form of this command to disable the function.

reset-button factory enable

no reset-button factory

Parameters

None.

Default

By default, this function is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the factory reset state of the reset button on the Switch. When enabled, pressing the reset button on the Switch more than 10 seconds will reset the Switch to factory defaults.

Example

This example shows how to disable the factory reset state of the reset button on the Switch.

```
Switch#configure terminal
Switch(config)#no reset-button factory
Switch(config)#
```

87. Route Map Commands

87-1 match interface

This command is used to define a clause to match the route's outgoing interface. Use the **no** form of this command to remove the clause.

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 configuration 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)#
```

87-2 match ip address

This command is used to define a clause to match the route based on the standard IP access list or IP prefix list. Use the **no** form of this command to remove the clause.

match ip address *ACCESS-LIST-NAME*

no match ip address *ACCESS-LIST-NAME*

Parameters

ACCESS-LIST-NAME	Specifies a standard or an extended 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 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 0.0.255.255 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)#
```

87-3 match ip next-hop

This command is used to define a clause to match the route’s next hop based on the standard IP access list or IP prefix list. Use the **no** form of this command to remove the clause.

match ip next-hop *ACCESS-LIST-NAME*

no match ip next-hop *ACCESS-LIST-NAME*

Parameters

ACCESS-LIST-NAME	Specifies the IP access list name.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command 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.

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 10.20.0.0 0.0.255.255
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)#
```

87-4 match ip route-source

This command is used to define a clause to match the route’s source router IP address based on the standard IP access list. Use the **no** form of this command to remove the clause.

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 0.0.255.255
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)#
```

87-5 match ipv6 address

This command is used to define a clause to match the route based on the standard IPv6 access list. Use the **no** form of this command to remove the clause.

match ipv6 address *ACCESS-LIST-NAME*

no match ipv6 address *ACCESS-LIST-NAME*

Parameters

ACCESS-LIST-NAME	Specifies a standard or an extended IPv6 access list name.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to define a rule for matching routes against an IPv6 access list.

Example

This example shows how to create an IPv6 access list “myacl6” first and create a route map entry to match against the IPv6 access list.

```
Switch#configure terminal
Switch(config)#ipv6 access-list myacl6
Switch(config-ipv6-acl)#permit 1000::/64
Switch(config-ipv6-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 address myacl6
Switch(config-route-map)#
```

87-6 match ipv6 next-hop

This command is used to define a clause to match the route’s next hop based on the standard IPv6 access list. Use the **no** form of this command to remove the clause.

match ipv6 next-hop *ACCESS-LIST-NAME*

no match ipv6 next-hop *ACCESS-LIST-NAME*

Parameters

ACCESS-LIST-NAME	Specifies the IPv6 access list name.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to define a rule for matching routes against the next hop. The IP address of the next hop will be matched against the IPv6 standard access list.

Example

This example shows how to create an IPv6 access list “myacl6” first and create a route map entry to match against the next hop based on the IPv6 access list.

```
Switch#configure terminal
Switch(config)#ipv6 access-list myacl6
Switch(config-ipv6-acl)#permit 1000::/64 any
Switch(config-ipv6-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 next-hop myacl6
Switch(config-route-map)#
```

87-7 match metric

This command is used to define a clause to match the route’s metric. Use the **no** form of this command to remove the clause.

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)#
```

87-8 match route-type

This command is used to define a clause to match the type of OSPF routes. Use the **no** form of this command to remove the clause.

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)#
```

87-9 route map

This command is used to create a route map rule entry. Use the **no** form of this 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)#
```

87-10 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/Privileged EXEC 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 mypolicy, permit, sequence 1
  Match clauses:
    ip address myacl
  Set clauses:
    next-hop 100.1.1.1

Total Entries: 1

Total Route Map Counts : 1
Switch#
```

87-11 set ip default next-hop

This command is used to configure the default next-hop of routers to route the packets that passes the match clauses of the configured route-map sequences. Use the **no** form of this 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 default 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 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)#
```

87-12 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** form of this command to remove the specified next-hop.

set ip next-hop {*IP-ADDRESS* **[***…IP-ADDRESS***] | recursive** *IP-ADDRESS***}**

no set ip next-hop {*IP-ADDRESS* **[***…IP-ADDRESS***] | recursive** *IP-ADDRESS***}**

Parameters

IP-ADDRESS	Specifies the IP address of the next-hop to route the packet.
recursive	Specifies the IP address of the recursive as the next-hop router.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command 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 is down, the second next-hop router in the list is responsible to route packets.

The recursive next-hop IP address is installed in the routing table and can be in a subnet that is not directly connected to it. If the recursive next-hop IP address is not available, a default route is used to route packets.

If both a next-hop and a recursive next-hop IP address are in the same route-map entry, the next-hop IP address is used. If the next-hop IP address is not available, the recursive next-hop IP address is used.

If other set clauses are used with the command for policy-based routing, they are evaluated in the following order:

1. **set ip next-hop**
2. **set ip default next-hop**

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)#
```

87-13 set ip precedence

This command is used to configure the precedence value in the IP header. Use the **no** form of this 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)#
```

87-14 set ipv6 default next-hop

This command is used to configure the default next-hop of routers to route the packets that passes the match clauses of the configured route-map sequences. Use the **no** form of this command to remove specific default next-hops.

set ipv6 default next-hop *IPV6-ADDRESS* **[***…IPV6-ADDRESS***]**

no set ipv6 default next-hop *IPV6-ADDRESS* **[***…IPV6-ADDRESS***]**

Parameters

IPV6-ADDRESS	Specifies the IPv6 address for the default next-hop to route the packet.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used for the IPv6 policy-based route. 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 the default next-hop of routers to route the packets that passes the match clauses of the configured route-map sequences.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ipacl1
Switch(config-ip-acl)#permit 1000::/64 any
Switch(config-ip-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 address ipacl1
Switch(config-route-map)#set ipv6 default next-hop 2000::1
Switch(config-route-map)#exit
Switch(config)#interface vlan1
Switch(config-if)#ip policy route-map mypolicy
Switch(config-if)#
```

87-15 set ipv6 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** form of this command to remove the clause.

set ipv6 next-hop {*IPV6-ADDRESS* **[***…IPV6-ADDRESS***] | recursive** *IPV6-ADDRESS***}**

no set ipv6 next-hop {*IPV6-ADDRESS* **[***…IPV6-ADDRESS***] | recursive** *IPV6-ADDRESS***}**

Parameters

IPV6-ADDRESS	Specifies the IPv6 address of the next-hop to route the packet.
recursive	Specifies the IP6 address of the recursive as the next-hop router.

Default

None.

Command Mode

Route-map Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify multiple IPv6 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 is down, the second next-hop router in the list is responsible to route packets.

The recursive next-hop IPv6 address is installed in the routing table and can be in a subnet that is not directly connected to it. If the recursive next-hop IPv6 address is not available, a default route is used to route packets.

If both a next-hop and a recursive next-hop IPv6 address are in the same route-map entry, the next-hop IPv6 address is used. If the next-hop IPv6 address is not available, the recursive next-hop IPv6 address is used.

If other set clauses are used with the command for policy-based routing, they are evaluated in the following order:

1. **set ipv6 next-hop**
2. **set ipv6 default next-hop**

Example

This example shows how to configure the next-hop router to route the packet that passes the match clauses of the configured route map sequence.

```
Switch#configure terminal
Switch(config)#ipv6 access-list ipacl1
Switch(config-ipv6-acl)#permit 1000::/64 any
Switch(config-ipv6-acl)#exit
Switch(config)#route-map mypolicy permit 1
Switch(config-route-map)#match ipv6 address ipacl1
Switch(config-route-map)#set ipv6 next-hop 2000::1
Switch(config-route-map)#
```

87-16 set ipv6 precedence

This command is used to configure the precedence value in the IPv6 header. Use the **no** form of this command to remove the setting.

set ipv6 precedence {*NUMBER* **|** *NAME***}**

no set ipv6 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 IPv6 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 IPv6 header. This command only takes effect when policy routing involves the IPv6 packet. The precedence can be set using either a number or the corresponding name.

Example

This example shows how to configure the IPv6 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 ipacl1
Switch(config-route-map)#set ipv6 precedence 5
Switch(config-route-map)#
```

87-17 set metric

This command is used to modify the metric of routes. Use the **no** form of this command to revert to the default setting.

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)#
```

87-18 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)#
```

88. Router Advertisement (RA) Guard Commands

88-1 ipv6 nd raguard policy

This command is used to create an Router Advertisement (RA) guard policy. The command will enter into the RA guard policy configuration mode. Use the **no** form of this command to remove an RA guard policy.

ipv6 nd raguard policy *POLICY-NAME*

no ipv6 nd raguard policy *POLICY-NAME*

Parameters

POLICY-NAME	Specifies the IPv6 RA guard policy name.

Default

None.

Command Mode

Global Configuration Mode.

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)#
```

88-2 device-role

This command is used to configure the role of the attached device. Use the **no** form of this command to revert to the default setting.

device-role {host | router}

no device-role

Parameters

host	Specifies to set the role of the attached device to host.
router	Specifies to set the role of the attached device to router.

Default

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

Command Mode

RA Guard Policy Configuration Mode.

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)#
```

88-3 match ipv6 access-list

This command is used to filter the RA messages based on the sender IPv6 address. Use the **no** form of this command to disable the filtering.

match ipv6 access-list *IPV6-ACCESS-LIST-NAME*

no match ipv6 access-list

Parameters

IPV6-ACCESS-LIST-NAME	Specifies a standard IPv6 access list.

Default

None.

Command Mode

RA Guard Policy Configuration Mode.

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)#
```

88-4 ipv6 nd raguard attach-policy

This command is used to apply an RA guard policy on a specified interface. Use the **no** form of this command to remove the binding.

ipv6 nd raguard attach-policy [*POLICY-NAME***]**

no ipv6 nd raguard

Parameters

POLICY-NAME	(Optional) 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 no parameter is specified, the default policy will set the device role to **host**.

Example

This example shows how to apply the RA guard policy on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#ipv6 nd raguard attach-policy raguard1
Switch(config-if)#
```

88-5 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display RA guard policy information. If no parameter is specified, information of all policies will be displayed for all policies.

Example

This example shows how to display the information of the RA guard policy “raguard1”.

```
Switch(config)#show ipv6 nd raguard policy raguard1

Policy raguard1 configuration:
    Device Role: host
    Source Address Match Access List: list1
    Target: eth1/0/3

Switch(config)#
```

89. Routing Information Protocol (RIP) Commands

89-1 default-metric (RIP)

This command is used to configure the value to be used as the default metric for routes redistributed to RIP. Use the **no** form of this command to revert to the default setting.

default-metric *METRIC-VALUE*

no default-metric

Parameters

METRIC-VALUE	Specifies the default metric value. The valid range of values is from 0 to 16.

Default

By default, this value is 0.

Command Mode

Router Configuration 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)#
```

89-2 distance (RIP)

This command is used to define an administrative distance of routes learned by IPv4 routing protocols. Use the **no** form of this command to revert to the default setting.

distance *DISTANCE*

no distance

Parameters

DISTANCE	Specifies the administrative distance. The range is from 1 to 255. The lower value represents a better route.

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 255 representing the trust rating of the route. The route with lower distance value is preferred over the route with the higher distance value.

Example

This example shows how to configure the distance of RIP routes to 100.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#distance 100
Switch(config-router)#
```

89-3 ip rip authentication mode

This command is used to specify the type of authentication used in RIP version 2 packets. Use the **no** form of this 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)#
```

89-4 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. Use the **no** form of this command to disable authentication.

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)#
```

89-5 ip rip receive version

This command is used to specify a RIP version to receive on an interface basis. Use the **no** form of this 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)#
```

89-6 ip rip send version

This command is used to specify a RIP version to send on an interface basis. Use the **no** form of this 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)#
```

89-7 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 this 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)#
```

89-8 network

This command is used to specify a network as one that runs RIP. Use the **no** form of this command to remove an entry.

network *NETWORK-PREFIX*

no network *NETWORK-PREFIX*

Parameters

NETWORK-PREFIX	Specifies 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)#
```

89-9 passive-interface

This command is used to disable the sending 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 all 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, routing updates are sent.

Command Mode

Router Configuration Mode.

Router Address Family Configuration (RIP) Mode.

Command Default Level

Level: 12.

Usage Guideline

If you disable the sending of routing updates on an interface, the router will not send 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 of routing updates on the interface VLAN 1.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#passive-interface vlan1
Switch(config-router)#
```

89-10 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** *METRIC-VALUE***] [route-map** *MAP-NAME***]**

Parameters

PROTOCOL	Specifies the protocol whose routes are to be redistributed. It can be one of the following keywords: **connected**, **ospf**, and **static**. 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, the original metric from the redistributed protocol will be transparently carried through.

If a route map is configured but the route map does not exist, it means all routes are not permitted. If a route map sequence has no match entry defined, 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 OSPF-derived metric will be remapped to 10.

```
Switch#configure terminal
Switch(config)#router rip
Switch(config-router)#redistribute ospf  metric 10
Switch(config-router)#
```

89-11 router rip

This command is used to configure the RIP routing process. Use the **no** form of this command to disable the RIP routing process.

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)#
```

89-12 show ip rip database

This command is used to display the RIP routing database.

show ip rip database [*IP-ADDRESS MASK* **|** *NETWORK-PREFIXIPREFIX–LENGTH***]**

Parameters

IP-ADDRESS MASK	(Optional) Specifies the address of the routing information that should be displayed.
NETWORK-PREFIXIPREFIX-LENGTH	(Optional) Specifies the subnet prefix and the prefix length of the network to be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to display the entry in the RIP routing database.

Example

This example shows how to display the RIP routing database.

```
Switch#show ip rip database

Codes: R - RIP, Rc - RIP connected, K - Kernel,
       C - Connected, S - Static, O - OSPF, A - Aggregate

    Network            Next Hop        Metric  From            If       Time

Rc  11.0.0.0/8                           1                   vlan11
R   105.100.0.0/24     11.0.0.5          2     11.0.0.5        vlan11   0DT0H0M2S
Rc  107.100.0.0/16                       1                   vlan1
R   212.254.254.0/24   11.0.0.254        2     11.0.0.254      vlan11   0DT0H0M10S

Total Entries: 4 entries, 4 routes
Switch#
```

89-13 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/Privileged EXEC Mode.

Command Default Level

Level: 12.

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

vlan11 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: none
    Passive interface: Disabled
    IP interface address:
      11.0.0.3/8

vlan1 is up, line protocol is up:
  Routing Protocol: RIP
    Receive RIP packets
    Send RIP packets
    Send v2-broadcast: Disabled
    Authentication Mode: none
    Passive interface: Disabled
    IP interface address:
      107.100.0.1/16

Total Entries : 2
Switch#
```

89-14 timers basic

This command is used to configure the RIP network timers. Use the **no** form of this command to revert to the default setting.

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)#
```

89-15 version

This command is used to specify a RIP version globally as the default version for all interfaces. Use the **no** form of this 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)#
```

90. Routing Information Protocol Next Generation (RIPng) Commands

90-1 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#
```

90-2 default-metric (RIPng)

This command is used to set the value used as the default metric for routes redistributed to RIPng. Use the **no** form of this command to revert to the default setting.

default-metric *METRIC-VALUE*

no default-metric

Parameters

METRIC-VALUE	Specifies the default metric value. The valid value is from 0 to 16.

Default

By default, this value is 0.

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, 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)#
```

90-3 distance (RIPng)

This command is used to define an administrative distance of routes learned by RIPng. Use the **no** form of this command to revert to 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 1 to 254 representing the trust rating of the route. The route with a lower distance value is preferred over the route with the higher distance value.

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)#
```

90-4 ipv6 rip enable

This command is used to enable an IPv6 RIP routing process on an interface. Use the **no** form of this command to disable an IPv6 RIP routing process on an interface.

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)#
```

90-5 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 this command to revert to 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)#
```

90-6 ipv6 router rip

This command is used to configure the IPv6 RIP routing process. Use the **no** form of this command to remove an IPv6 RIP routing process.

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)#
```

90-7 poison-reverse

This command is used to enable the poison reverse processing for an IPv6 RIP process. Use the **no** form of this 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)#
```

90-8 redistribute (RIPng)

This command is used to redistribute routes from other routing domains into RIP. Use the **no** form of this 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. It can be one of the following keywords: **connected**, **ospf**, and **static**. The **static** keyword means to redistribute IPv6 static routes. The **connected** keyword refers to routes that are established automatically by virtue of configuring IPv6 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, the original metric from the redistributed protocol will be transparently carried through.

Example

This example shows how to configure the OSPF 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)#
```

90-9 passive-interface

This command is used to disable the sending of the routing updates on an interface. Use the **no** form of this command to revert to the default setting.

passive-interface {default | *INTERFACE-ID***}**

no passive-interface {default | *INTERFACE-ID***}**

Parameters

default	Specifies the global default passive state for the interface.
INTERFACE-ID	Specifies an interface to be used.

Default

By default, routing updates are sent.

Command Mode

Router Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If this option is disabled, the router will not send RIPng packet out through the interface. However, RIPng packets from other routers received on the interface will continue to be processed.

Example

This example shows how to disable the sending of the routing updates on an interface.

```
Switch#configure terminal
Switch(config)#ipv6 router rip
Switch(config-rtr)#passive-interface vlan1
Switch(config-rtr)#
```

90-10 show ipv6 rip

This command is used to display interface information of RIPng.

show ipv6 rip [database]

Parameters

database	(Optional) Specifies to display the entry in the RIP routing database.

Default

None.

Command Mode

User/Privileged EXEC 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 entries in the RIPng 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 120
     Updates every 30 seconds, expire after 180 seconds
     Garbage collect after 120 seconds
     Split horizon is on; poison reverse is off
     Periodic updates 44, trigger updates 1

  Interfaces:
     vlan1
     vlan2
     vlan3
  Redistribution:
     Redistributing static with metric 2

Switch#
```

90-11 split-horizon

This command is used to enable the split-horizon option for an IPv6 RIP process. Use the **no** form of this 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)#
```

90-12 timers

This command is used to configure the IPv6 RIP network timers. Use the **no** form of this command to revert to the default setting.

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)#
```

90-13 debug ipv6 rip

This command is used to turn on the IPv6 RIP debug function. Use the **no** form of this command to turn off the IPv6 RIP debug function.

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#
```

90-14 debug ipv6 rip interface

This command is used to turn on the IPv6 RIP interface state debug switch. Use the **no** form of this command to turn off the IPv6 RIP interface state debug switch.

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
```

90-15 debug ipv6 rip packet-transmitting

This command is used to turn on the IPv6 RIP packet transmitting debug switch. Use the **no** form of this command to turn off the IPv6 RIP packet transmitting debug switch.

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 FF02::9 , Index 1
```

90-16 debug ipv6 rip packet-receiving

This command is used to turn on the IPv6 RIP packet receiving debug switch. Use the **no** form of this command to turn off the IPv6 RIP packet receiving debug switch.

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
```

90-17 debug ipv6 rip route

This command is used to turn on the IPv6 RIP route debug switch. Use the **no** form of this command to turn off the IPv6 RIP route debug switch.

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#
Switch#
 Add a RIPng route to V6 route table dst= 2016:3630:: nexthop= FE80::206:28FF:FED8:FEAC

Switch#
Switch#
```

91. Safeguard Engine Commands

91-1 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, 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, all protocols will be cleared.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to clear the CPU protect related counters.

Example

This example shows how to clear all CPU protect related statistics.

```
Switch#clear cpu-protect counters all
Switch#
```

91-2 cpu-protect safeguard

This command is used to enable or configure the Safeguard Engine. Use the **no** form of this command to disable the Safeguard Engine

cpu-protect safeguard [threshold *RISING-THRESHOLD FALLING-THRESHOLD***]**

no cpu-protect safeguard [threshold]

Parameters

threshold	(Optional) Specifies to configure the utilization to control when the Safeguard Engine function will activate.
RISING-THRESHOLD	(Optional) Specifies to set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises over

	the specified percentage, the Safeguard Engine mechanism will initiate. The valid range is from 20 to 100.
FALLING-THRESHOLD	(Optional) Specifies to set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to the specified percentage, the Safeguard Engine mechanism will shut down. The valid range is from 20 to 100.

Default

By default, Safeguard Engine is disabled.

By default, the rising threshold of CPU utilization is 50.

By default, the falling threshold of CPU utilization is 20.

Command Mode

Global Configuration Mode.

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)#
```

91-3 cpu-protect sub-interface

This command is used to configure the rate limit for traffic destined for the CPU by sub-interface types. Use the **no** form of this command to revert to the default settings.

cpu-protect sub-interface {manage | protocol | route} pps *RATE*

no cpu-protect sub-interface {manage | protocol | route}

Parameters

pps *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 for 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)#
```

91-4 cpu-protect type

This command is used to configure the rate limit of traffic destined for the CPU by the protocol type. Use the **no** form of this command to revert to the default setting.

cpu-protect type *PROTOCOL-NAME* **pps** *RATE*

no cpu-protect type *PROTOCOL-NAME*

Parameters

PROTOCOL-NAME	Specifies the protocol name to be configured.
pps *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 for 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 for CPU, the router creates three virtual sub-interfaces to process the packets:

- **manage -** The packets are destined for 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.



NOTE: The CPU will check if the receiving packet contains a protocol virtual sub-interface first. Then, the CPU will check if the receiving packet contains a manage virtual sub-interface. If the packet does not contain a protocol or a manage virtual sub-interface, it will be classified as a route virtual sub-interface.

The following table lists the supported protocol names for this command:

Protocol Name	Description	Classification (sub-interface)
8021x	Port-based Network Access Control	Protocol
arp	IP Address Resolution Protocol (ARP)	Protocol
dhcp	Dynamic Host Configuration	Protocol
dns	Domain Name Services	Protocol
dvmrp	Distance Vector Multicast Routing Protocol	Protocol
gvrp	GARP VLAN Registration Protocol	Protocol
icmpv4	IPv4 Internet Control Message Protocol	Protocol
icmpv6-nighbor	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
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)#
```

91-5 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/Privileged EXEC 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.

91-6 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 stacking unit ID to display the rate limit configuration and statistics by sub-interface. This parameter is only available when the stacking mode is enabled.

Default

None.

Command Mode

User/Privileged EXEC 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: 10 pps

Unit  Total                          Drop
----- ------------------------------ ------------------------------
1     103                            12

Switch#
```

91-7 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 will be displayed if the optional unit ID is not specified. Otherwise, only the information on the specified unit ID will be displayed. The *UNIT-ID* parameter is only available when the stacking mode is enabled.
unit *UNIT-ID*	Specifies the unit ID to display the rate limit configuration and statistics. This parameter is only available when the stacking mode is enabled.

Default

None.

Command Mode

User/Privileged EXEC 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 dhcp

Type: dhcp
Rate Limit: 200 pps

Unit  Total                          Drop
----- ------------------------------ ------------------------------
1     0                              0

Switch#
```

91-8 snmp-server enable traps safeguard-engine

This command is used to enable the sending of SNMP notifications for the Safeguard Engine. Use the **no** form of this command to disable the sending of SNMP notifications for the Safeguard Engine.

snmp-server enable traps safeguard-engine

no snmp-server enable traps safeguard-engine

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of SNMP notifications when the current mode of Safeguard Engine changes.

Example

This example shows how to enable traps for the current mode of the Safeguard Engine change event.

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

92. Secure File Transfer Protocol (SFTP) Client Commands

92-1 ip ssh client authmethod

This command is used to configure the SFTP client authentication method on the Switch. Use the **no** form of this command to revert to the default setting.

ip ssh client authmethod {password | publickey}

no ip ssh client authmethod

Parameters

password	Specifies to use password as the SFTP client authentication method.
publickey	Specifies to use public key as the SFTP client authentication method.

Default

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

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the SFTP client authentication method on the Switch.

Current supported ciphers of the SFTP client are:

- Key exchange algorithms : diffie-hellman-group1-sha1
- MAC algorithms : hmac-sha1
- Encryption algorithms : 3des-cbc

When configuring **password** as the SFTP client authentication method, use the following steps to successfully connect to the SFTP server.

1. Use the **ip ssh client authmethod password** command on the Switch.
2. Configure the username and password on the SFTP server.
3. Use the **copy** command to download/upload files from/to the SFTP server. Username and password are required when connecting to the SFTP server.

When configuring **publickey** as the SFTP client authentication method, use the following steps to successfully connect to the SFTP server.

1. Use the **ip ssh client authmethod publickey** command on the Switch.
2. Generate an RSA key pair. The Switch only supports RSA, 1024-bit length, and OpenSSH format.
3. Download the RSA key pair to the Switch.
4. Download the RSA public key to the SFTP server.
5. Configure the public key path on the SFTP server.
6. Use the **copy** command to download/upload files from/to the SFTP server. Username is required when connecting to the SFTP server.

Example

This example shows how to configure to use password as the SFTP client authentication method.

```
Switch#configure terminal
Switch(config)#ip ssh client authmethod password
Switch(config)#
```

92-2 ip ssh client keypath

This command is used to configure the secret key file path of the SFTP client. Use the **no** form of this command to clear the key path.

ip ssh client keypath {publickey *STRING* **| privatekey** *STRING***}**

no ip ssh client keypath {publickey | privatekey}

Parameters

publickey *STRING*	Specifies the public key file path of the SFTP client with a maximum of 200 characters.
privatekey *STRING*	Specifies the private key file path of the SFTP client with a maximum of 200 characters.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the secret key file path of the SFTP client. When **publickey** is used as the SFTP client authentication method, this command should be configured.

Example

This example shows how to configure the public key file path of the SFTP client.

```
Switch#configure terminal
Switch(config)#ip ssh client keypath publickey /c:/Identity.pub
Switch(config)#
```

92-3 show ip ssh client

This command is used to display the settings of the SFTP client.

show ip ssh client

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the settings of the SFTP client.

Example

This example shows how to display the settings of the SFTP client.

```
Switch#show ip ssh client

 auth method : Publickey
 Public key path  : /c:/Identity.pub
 Private key path : /c:/Identity

Switch#
```

93. Secure File Transfer Protocol (SFTP) Server Commands

93-1 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)#
```

93-2 ip sftp timeout

This command is used to configure the SFTP idle timer on the Switch. Use the **no** form of this command to revert to the default setting.

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)#
```

93-3 show ip sftp

This command is used to display the SFTP server settings.

show ip sftp

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

94. Secure Shell (SSH) Commands

94-1 crypto key generate

This command is used to generate the RSA or DSA key pair.

crypto key generate {rsa [modulus *MODULUS-SIZE***] | dsa}**

Parameters

rsa	Specifies to generate the RSA key pair.
modulus *MODULUS-SIZE*	(Optional) Specifies the number of bits in the modulus. For RSA, the valid values are 360, 512, 768, 1024, and 2048.If not specified, a message will be promoted to the user to specify the value.
dsa	Specifies to generate the DSA key pair. The DSA key size is fixed as 1024 bit.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

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#
```

94-2 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: 15.

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#
```

94-3 ip ssh timeout

This command is used to configure the SSH control parameters on the Switch. Use the **no** form of this command to revert to the default setting.

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)#
```

94-4 ip ssh server

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

ip ssh server

no ip ssh server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the SSH server function.

Example

This example shows how to enable the SSH server function.

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

94-5 ip ssh service-port

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

ip ssh service-port *TCP-PORT*

no ip ssh service-port

Parameters

TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the SSH protocol is 22.

Default

By default, this value is 22.

Command Mode

Global Configuration Mode.

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)#
```

94-6 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to display the RSA or DSA public key pairs.

Example

This example shows how to display the information of the RSA public key.

```
Switch#show crypto key mypubkey rsa

% Key pair was generated at: 09:48:40, 2013-11-29
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AADAQAB AAAAQwCN 6IRFHCBf jsHvYjQG iCL0p2kz 2v38ULC8
kAKra/Ze mG7IW3eC 8STcrkr5 s719H/bh jG/oqkwj SlUJSGqR e/sj6Ws=

Switch#
```

94-7 show ip ssh

This command is used to display the user SSH configuration settings.

show ip ssh

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the SSH configuration settings.

Example

This example shows how to display the SSH configuration settings.

```
Switch#show ip ssh

IP SSH server              : Enabled
IP SSH service port        : 22
SSH server mode            : V2
Authentication timeout     : 120 secs
Authentication retries     : 3 times

Switch#
```

94-8 show ssh

This command is used to display the status of SSH server connections.

show ssh

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the status of SSH server connections on the Switch.

Example

This example shows how to display the status of SSH server connections.

```
Switch#show ssh

SID Ver. Cipher                       Userid           Client IP Address
--- --- ---------------------------- ---------------- -------------------------
0   V2  3des-cbc/hmac-sha1-96        zhang3           192.168.0.100
1   V2  3des-cbc/hmac-sha1           lee4567890123456 2000::243

Total Entries: 2

Switch#
```

Display Parameters

SID	A unique number that identifies the SSH session.
Ver	Indicates the SSH version of this session.
Cipher	The cryptographic / Hashed Message Authentication Code (HMAC) algorithm that the SSH client is using.
Userid	The login username of the session.
Client IP Address	The client IP address for this established SSH session.

94-9 ssh user authentication-method

This command is used to configure the SSH authentication method for a user account. Use the **no** form of this command to revert to the default settings.

ssh user *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

no ssh user *NAME* **authentication-method**

Parameters

NAME	Specifies the username to configure the authentication type. The user must be an existing local account. The length of the username is limited to a maximum of 32 characters.
password	Specifies to use the password authentication method for this user account. This is the default authentication method.
publickey *URL*	Specifies to use the public key authentication method for this user account. Enter the URL of a local file to be used as the public key of this user.
hostbased *URL*	Specifies to use the host-based authentication method for this user account. Enter the URL of a local file to be used as client's host key.
host-name *HOSTNAME*	Specifies the allowed host name for host-based authentication. During authentication phase, the client's hostname will be checked. The range is from 1 to 255.
IP-ADDRESS	(Optional) Specifies whether to additionally check the IP address of the client for host-based authentication. If the IPv4/IPv6 address is 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 the IPv4/IPv6 address is 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: 15.

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 log into 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 user1 authentication-method publickey c:/user1.pub
Switch(config)#
```

95. sFlow Commands

95-1 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 revert one receiver to the default settings.

sflow receiver *INDEX* **[owner** *NAME***] [expiry {***SECONDS* **| infinite}] [max-datagram-size** *SIZE***] [host {***IP-ADDRESS* **|** *IPV6-ADDRESS***}] [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.
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)#
```

95-2 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 this parameter is 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 this parameter is 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 this parameter is 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 eth1/0/1
Switch(config-if)#sflow sampler 1 receiver 1 inbound sampling-rate 1024 max-header-size 128
Switch(config-if)#
```

95-3 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 this parameter is 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 this parameter is 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 eth1/0/1
Switch(config-if)#sflow poller 1 receiver 1 interval 20
Switch(config-if)#
```

95-4 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/Privileged EXEC 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       : 1.3;D-Link Corporation Inc.;1.00
sFlow Agent Address       : 10.90.90.91
sFlow Agent IPv6 Address  :

Receivers Information
Index                     : 1
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 2
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 3
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Index                     : 4
Owner                     :
Expire Time               : 0
Current Countdown Time    : 0
Max Datagram Size         : 1400
Address                   : 0.0.0.0
Port                      : 6343
Datagram Version          : 5

Samplers Information
Interface Instance Receiver   Mode   Admin Rate  Active Rate  Max Header Size
--------- -------- -------- -------- ----------  -----------  ---------------

Pollers Information
Interface  Instance  Receiver  Interval
---------  --------  --------  --------


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 expiration 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.
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.

96. Simple Mail Transfer Protocol (SMTP) Commands

96-1 smtp server

This command is used to configure the SMTP server and port setting. Use the **no smtp server** command to clear the SMTP server. Use the **no smtp server port** command to revert the port to the default setting.

smtp server {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [port** *PORT***]**

no smtp server

no smtp server port

Parameters

IP-ADDRESS	Specifies the IPv4 address of the SMTP server.
IPV6-ADDRESS	Specifies the IPv6 address of the SMTP server.
port *PORT*	(Optional) Specifies the TCP port number used to contact the SMTP server. The valid range is from 1 and 65535.

Default

By default, no server address is configured.

By default, the port number 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. When the Switch acts as the SMTP client and sends the SYSLOG message to the SMTP server, 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 port 587
Switch(config)#
```

96-2 smtp self

This command is used to configure the email address which represents the Switch that sends the email message. Use the **no** form of this command to remove the email address that represents the Switch.

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)#
```

96-3 smtp recipient

This command is used to configure the recipient where the email will be sent. Use the **no** form of this command to remove a recipient.

smtp recipient *EMAIL-ADDRESS*

no smtp recipient {all | *EMAIL-ADDRESS***}**

Parameters

EMAIL-ADDRESS	Specifies a recipient to receive the email.
all	Specifies all recipients to be removed.

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)#
```

96-4 smtp interval

This command is used to configure the SMTP interval time. Use the **no** form of this command to revert to the default setting.

smtp interval *MINUTES*

no smtp interval

Parameters

MINUTES	Specifies the SMTP sending interval. If set to 0, the 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)#
```

96-5 show smtp

This command is used to display SMTP information.

show smtp

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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 IPv4 Server Address: 172.18.50.9
SMTP IPv4 Server Port   : 25
SMTP IPv6 Server Address: 2000::91
SMTP IPv6 Server Port   : 65535
Self Mail Address       : switch@domain.com
Send Interval           : 0

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#
```

96-6 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.



NOTE: The ENTER key is used to indicate the end of the text entered in the Subject and Content fields.

```
Switch# smtp send-testmsg

Subject:This is a test of smtp
Content:Hello, everybody!

Sending mail, please wait...
< send line, > receive line, [] message
[Trying to connect IPv4 server......]
[Connect to IPv4 server 10.1.1.1 port 25]
>220 mail.test.com ESMTP MAIL Service ready at Thu, 16 Oct 2022 13:59:30 +0800
<HELO Switch
>250 mail.test.com Hello [10.90.90.90]
<MAIL FROM:<sender@test.com>
>250 2.1.0 Sender OK
<RCPT TO:<reciever@test.com >
>250 2.1.5 Recipient OK
<DATA
>354 Start mail input; end with <CRLF>.<CRLF>
<From: sender@test.com
<To: reciever@test.com
<Subject: Test mail from DGS-1520 : This is a test of smtp
<
From device DGS-1520 10.90.90.90
<Oct 16 2022 05:59:44.470
<
<Hello, everybody!
<
<.
>250 2.6.0 <8d54887926b140a3958e5bc0f7382f52@mail.test.com> [InternalId=13421772800270,
Hostname=mail.test.com] Queued mail for delivery
<QUIT
Switch#
```

97. Simple Network Management Protocol (SNMP) Commands

97-1 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/Privileged EXEC 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

Community : public
 Access : read-only
 View : CommunityView

Community : private
 Access : read-write
 View : CommunityView

Total Entries: 2

Switch#
```

This example shows how to display the SNMP server host setting.

```
Switch#show snmp host

Host IP Address  : 10.90.90.1
SNMP Version     : V1
Community Name   : public
UDP Port         : 162

Total Entries: 1

Switch#
```

This example shows how to display the MIB view setting.

```
Switch#show snmp view

restricted(included) 1.3.6.1.2.1.1
restricted(included) 1.3.6.1.2.1.11
restricted(included) 1.3.6.1.6.3.10.2.1
restricted(included) 1.3.6.1.6.3.11.2.1
restricted(included) 1.3.6.1.6.3.15.1.1
CommunityView(included) 1
CommunityView(excluded) 1.3.6.1.6.3
CommunityView(included) 1.3.6.1.6.3.1

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

This example shows how to display the SNMP engine ID.

```
Switch#show snmp engineID

Local SNMP engineID: 800000ab03f07d6834001000

Switch#
```

97-2 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/Privileged EXEC 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 to display SNMP users.

```
Switch#show snmp user

User Name: initial
  Security Model: 3
  Group Name: initial
  Authentication Protocol: None
  Privacy Protocol: None
  Engine ID: 800000ab03f07d6834001000
  IP access control list:

Total Entries: 1

Switch#
```

97-3 snmp-server community

This command is used to configure the community string to access the SNMP. Use the **no** form of this command to remove the community string.

snmp-server community [0 | 7] *COMMUNITY-STRING* **[view** *VIEW-NAME***] [ro | rw] [access** *IP-ACL-NAME***] [context** *CONTEXT***]**

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. The hash symbol (#) is not allowed in the string.
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.
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.
context *CONTEXT*	(Optional) Specifies the SNMP context name.

Default

Community	View Name	Access right

private	CommunityView	Read/Write
public	CommunityView	Read Only

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command provides an easy way to create a community string for SNMPv1 and SNMPv2c management. When creating a community with the **snmp-server community** command, two SNMP group entries, one for SNMPv1 and one for SNMPv2c, which has the community name as their group names are created. If **view** is not specified, it is permitted to access all objects.

Example

This example shows how 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 1.3.6.1.2.1.2 included
Switch(config)#snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

97-4 snmp-server engineID local

This command is used to specify the SNMP engine ID on the local device. Use the **no** form of this command to revert to the default setting.

snmp-server engineID local *ENGINEID-STRING*

no snmp-server engineID local

Parameters

ENGINEID-STRING	Specifies the engine ID string of a maximum of 24 characters.

Default

A default SNMP engine ID is automatically generated.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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)#
```

97-5 snmp-server group

This command is used to configure an SNMP group. Use the **no** form of this command to remove a SNMP group or remove a group from using a specific security model.

snmp-server group *GROUP-NAME* **{v1 | v2c | v3 {auth | noauth | priv}} [read** *READ-VIEW***] [write** *WRITE-VIEW***] [notify** *NOTIFY-VIEW***] [access** *IP-ACL-NAME***] [context** *CONTEXT***]**

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.
context *CONTEXT*	(Optional) Specifies the SNMP context name.

Default

Group Name	Version	Security Level	Read View Name	Write View Name	Notify View Name
initial	SNMPv3	noauth	Restricted	None	Restricted
public	SNMPv1	None	CommunityView	None	CommunityView
public	SNMPv2c	None	CommunityView	None	CommunityView
private	SNMPv1	None	CommunityView	CommunityView	CommunityView
private	SNMPv2c	None	CommunityView	CommunityView	CommunityView

By default, no ACL is associated with any SNMP group.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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, 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, 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, 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)#
```

97-6 snmp-server host

This command is used to specify the recipient of the SNMP notification. Use the **no** form of this command to remove the recipient.

snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [version {1 | 2c | 3 {auth | noauth | priv}}]** *COMMUNITY-STRING* **[port** *PORT-NUMBER***]**

no snmp-server host {*IP-ADDRESS* **|** *IPV6-ADDRESS***} [***COMMUNITY-STRING***]**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the SNMP notification host.
IPV6-ADDRESS	Specifies the IPv6 address of the SNMP notification host.
version	(Optional) Specifies the version of the SNMP used to send the traps. If this parameter is not specified, the default is SNMPv1 **1** - SNMPv1. **2c** - SNMPv2c. **3** - SNMPv3.
auth	(Optional) Specifies to authenticate the packet but not to encrypt it.
noauth	(Optional) Specifies neither to authenticate nor to encrypt the packets.
priv	(Optional) Specifies to both authenticate and to encrypt the packet.

COMMUNITY-STRING	Specifies the community string to be sent with the notification packet. If the version is 3, the community string is used as the username as defined in the **snmp-sever user** command.
port *PORT-NUMBER*	(Optional) Specifies the UDP port number. The default trap UDP port number is 162. The range of UDP port numbers is from 1 to 65535. Some port numbers may conflict with other protocols.

Default

By default, the version used is 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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.

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)#
```

97-7 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. Use the **no** form of this command to revert to the default setting.

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: 15.

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 source-interface traps vlan100
Switch(config)#
```

97-8 snmp-server user

This command is used to create an SNMP user. Use the **no** form of this command to remove an SNMP user.

snmp-server user *USER-NAME GROUP-NAME* **[encrypted] [auth {md5 | sha}** *AUTH-PASSWORD* **[priv {des** *PRIV-PASSWORD* **| aes** *PRIV-PASSWORD***}]] [access** *IP-ACL-NAME***]**

no snmp-server user *USER-NAME GROUP-NAME*

Parameters

USER-NAME	Specifies a username of a maximum of 32 characters. The syntax is general string that does not allow spaces.
GROUP-NAME	Specifies the name of the group to which the user belongs. The syntax is general string that does not allow spaces.
encrypted	(Optional) Specifies that the following password is in encrypted format.
auth	(Optional) Specifies the authentication level.
md5	(Optional) Specifies to use HMAC-MD5-96 authentication.
sha	(Optional) Specifies to use HMAC-SHA-96 authentication.
AUTH-PASSWORD	(Optional) Specifies the authentication password in the plain-text form. This password is 8 to 16 octets for MD5 and 8 to 20 octets for SHA. If the **encrypted** parameter is specified, the length is 32 for MD5 and 40 for SHA. The format is a hexadecimal value.
priv	(Optional) Specifies the type of encryption.
des	(Optional) Specifies to use DES algorithm for encryption.
aes	(Optional) Specifies to use AES algorithm for encryption.
PRIV-PASSWORD	Specifies the private password in the plain-text form. This password can be up to 64 characters. If the **encrypted** parameter is specified, the length is fixed to 16 octets.
access *IP-ACL-NAME*	(Optional) Specifies the standard IP 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: 15.

Usage Guideline

To create an SNMP user, specify the security model that the user uses and the group that the user is created for. To create an SNMPv3 user, the password used for authentication and encryption needs to be specified.

An SNMP user is unable to be deleted if it has been associated with a SNMP server host.

Example

This example shows how to configure the plain-text password, authpassword, for the user, user1, in the SNMPv3 group public.

```
Switch#configure terminal
Switch(config)#snmp-server user user1 public auth md5 authpassword
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 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

97-9 snmp-server view

This command is used to create or modify a view entry. Use the **no** form of this command to remove a specified SNMP view entry.

snmp-server view *VIEW-NAME OID-TREE* **{included | excluded}**

no snmp-server view *VIEW-NAME*

Parameters

VIEW-NAME	Specifies the name of the view entry. The valid length is 1 to 32 characters. The syntax is general string that does not allow spaces.
OID-TREE	Specifies the object identifier of the ASN.1 sub-tree to be included or excluded from the view. To identify the sub-tree, specify a text string consisting of numbers, such as 1.3.6.2.4, or a word, such as system.
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: 15.

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 “interfacesMibView” as the read view.

```
Switch#configure terminal
Switch(config)#snmp-server view interfacesMibView 1.3.6.1.2.1.1.2 included
Switch(config)#snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

97-10 show snmp trap link-status

This command is used to display the per interface link status trap state.

show snmp trap link-status [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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 on ports 1 to 9.

```
Switch#show snmp trap link-status interface eth1/0/1-9

Interface           Trap state
-------------       -------------
eth1/0/1            Enabled
eth1/0/2            Enabled
eth1/0/3            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


Switch#
```

97-11 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/Privileged EXEC 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         : Switch
Location     :
Contact      :
SNMP UDP Port    : 161
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                : Disabled
    Warmstart                : Disabled

Switch#
```

97-12 show snmp-server trap-sending

This command is used to display the per port SNMP trap sending state.

show snmp-server trap-sending [interface *INTERFACE-ID* **[, | -]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the per port trap sending state. If no optional parameter is specified, all ports will be displayed.

Example

This example shows how to display the trap sending state on ports 1 to 9.

```
Switch#show snmp-server trap-sending interface eth1/0/1-9

       Port                          Trap Sending
-----------------                   ---------------
 eth1/0/1                              Enabled
 eth1/0/2                              Enabled
 eth1/0/3                              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
Switch#
```

97-13 snmp-server

This command is used to enable the SNMP agent. Use the **no** form of this command to disable the SNMP agent.

snmp-server

no snmp-server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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)#
```

97-14 snmp-server contact

This command is used to configure the system contact information for the device. Use the **no** form of this command to remove the setting.

snmp-server contact *TEXT*

no snmp-server contact

Parameters

TEXT	Specifies a string for describing the system contact information. The maximum length is 255 characters The syntax is a general string that allows spaces.

Default

None.

Command Mode

Global Configuration Mode.

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)#
```

97-15 snmp-server enable traps

This command is used to enable the sending of trap packets globally. Use the **no** form of this command to disable the sending of trap packets.

snmp-server enable traps

no snmp-server enable traps

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the device to send the SNMP notification traps globally.

Example

This example shows how to enable the SNMP traps global sending state.

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

97-16 snmp-server enable traps snmp

This command is used to enable the sending of all or specific SNMP notifications. Use the **no** form of this command to disable the sending of all or specific SNMP notifications.

snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

no snmp-server enable traps snmp [authentication] [linkup] [linkdown] [coldstart] [warmstart]

Parameters

authentication	(Optional) Specifies to control the sending of SNMP authentication failure notifications. An authenticationFailuretrap is generated when the device receives an SNMP message that is not properly authenticated. The authentication method depends on the version of SNMP being used. For SNMPv1 or SNMPv2c, authentication failure occurs if packets are formed with an incorrect community string. For SNMPv3, authentication failure occurs if packets are formed with an incorrect SHA/MD5 authentication key.
linkup	(Optional) Specifies to control the sending of SNMP linkUp notifications. A linkup (3) trap 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)#
```

97-17 snmp-server location

This command is used to configure the system's location information. Use the **no** form of this command to remove the setting.

snmp-server location *TEXT*

no snmp-server location

Parameters

TEXT	Specifies the string that describes the system location information. The maximum length is 255 characters. The syntax is a general string that allows spaces.

Default

None.

Command Mode

Global Configuration Mode.

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)#
```

97-18 snmp-server name

This command is used to configure the system's name information. Use the **no** form of this command to remove the setting.

snmp-server name *NAME*

no snmp-server name

Parameters

NAME	Specifies the string that describes the host name information. The maximum length is 255 characters. As a suggestion do not configure the hostname longer than 10 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

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)#snmp-server name SiteA-switch
SiteA-switch(config)#
```

97-19 snmp-server trap-sending disable

This command is used to disable the sending of notifications for the port. Use the **no** form of this command to enable the sending of notifications for the port.

snmp-server trap-sending disable

no snmp-server trap-sending disable

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to disable or enable the sending of notifications for the port. When disabled, SNMP notification traps generated by the system are not allowed to transmit out of the port. The SNMP traps generated by other system and forwarded to the port is not subject to this restriction.

Example

This example shows how to disable the sending of notifications for port 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#snmp-server trap-sending disable
Switch(config-if)#
```

97-20 snmp-server service-port

This command is used to configure the SNMP UDP port number. Use the **no** form of this command to revert to the default setting.

snmp-server service-port *PORT-NUMBER*

no snmp-server service-port

Parameters

PORT-NUMBER	Specifies the UDP port number. The range is from 1 to 65535. Some numbers may conflict with other protocols.

Default

By default, this number is 161.

Command Mode

Global Configuration Mode.

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)#
```

97-21 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)#
```

97-22 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#no snmp trap link-status
Switch(config-if)#
```

97-23 snmp-server context-map

This command is used to configure the SNMP context mapping table. Use the **no** form of this command to remove the configuration.

snmp-server context-map *CONTEXT* **[instance-id** *INT***] [instance-name** *NAME***]**

no snmp-server context-map *CONTEXT*

Parameters

CONTEXT	Specifies the VACM context name. This name can be up to 32 characters long.
instance-id *INT*	Specifies the instance ID of the protocol. The range is from 1 to 65535.
instance-name *NAME*	Specifies the instance name of the protocol. This name can be up to 12 characters long.

Default

By default, the VACM context name is Contex1.

By default, the instance ID is 0.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the SNMP context mapping table information on the Switch.

Example

This example shows how to configure the SNMP context to “snmp-context”.

```
Switch#configure terminal
Switch(config)#snmp-server context-map snmp-context
Switch(config)#
```

97-24 show snmp context-map

This command is used to display information about the configured SNMP context mapping table.

show snmp context-map

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display information about the configured SNMP context mapping table.

Example

This example shows how to display information about the configured SNMP context mapping table.

```
Switch#show snmp context-map

 SNMP Context Mapping Table:

Context Name : Context1
 Instance ID : 0
 Instance Name :


Switch#
```

98. Single IP Management (SIM) Commands

98-1 sim

This command is used to enable single IP management. Use the **no** form of this command to disable 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 or 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)#
```

98-2 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)#
```

98-3 sim group-member

This command is used to add one Candidate switch to the single IP management group. Use the **no** form of this command 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	(Optional) 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)#
```

98-4 sim holdtime

This command is used to configure the hold-time duration in seconds. One switch (either 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 of this command to revert to the default setting.

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)#
```

98-5 sim interval

This command is used to configure the SIM interval in seconds for single IP management protocol sending messages. Use the **no** form of this command to revert to the default setting.

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)#
```

98-6 sim management vlan

This command is used to configure SIM management VLAN. Use the **no** form of this 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)#
```

98-7 sim remote-config

This command is used to remotely log in and configure the single IP management group member or exit from the remote configuration.

sim remote-config {member *MEMBER-ID* **| exit}**

Parameters

member *MEMBER-ID*	Specifies the login member.
exit	Specifies to exit from the current configuring member.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

The SIM Commander switch can log into 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 configure the member ID.

```
Switch#sim remote-config member 1
Switch#
```

98-8 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 at 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 *MEMBER-LIST*	(Optional) Specifies the member switch to download the file. Multiple members can be specified at a time. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

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

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

ID   MAC Address       Status
---------------------------------------
1    00-02-01-03-01-03 SUCCESS

Switch#
```

98-9 snmp-server enable traps sim

This command is used to enable the sending of single IP management trap. Use the **no** form of this command to disable the state.

snmp-server enable traps sim

no snmp-server enable traps 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 or disable the sending of SIM traps.

Example

This example shows how to enable the SIM trap state.

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

98-10 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	(Optional) Specifies to display the information of Candidate switches.
CANDIDATE-ID	(Optional) Specifies to display detailed information of a Candidate.
members	(Optional) Specifies to display the information of Member switches.
MEMBER-ID	(Optional) Specifies to display detailed information of a Member.
group	(Optional) Specifies to display the information of other SIM Groups.
COMMANDER-MAC	(Optional) Specifies to display detailed information of a Group.
neighbor	(Optional) Specifies to display the neighbor information.

Default

None.

Command Mode

User/Privileged EXEC 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    : 1.01.004
    Management VLAN     : 1
    Device Name         : Switch
    MAC Address         : 80-26-89-15-28-00
    Platform            : DGS-1520-28MP
    SIM State           : Enabled
    Role State          : Commander
    Discovery Interval  : 30 sec
    Hold Time           : 100 sec
    Trap                : Disabled

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    : 1.01.004
    Device Name         :
    MAC Address         : 80-26-00-15-28-00
    Platform            : DGS-1520-28MP
    SIM State           : Enabled
    Role State          : Member
    Discovery Interval  : 30 sec
    Hold Time           : 100 sec
----------------CS Info----------------
    CS Group Name    : my-group
    CS MAC Address   : 80-26-89-15-28-00
    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    80-26-00-15-28-00 DGS-1520-28MP              100  1.01.004
  2    80-26-01-15-28-00 DGS-1520-28MP               80  1.01.004

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      : 1.01.004
    Device Name           :
    MAC Address           : 80-26-00-15-28-00
    Platform              : DGS-1520-28MP
    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 DGS-1520-28MP              90  1.01.004

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      : 1.01.004
 Device Name           :
 MAC Address           : EE-FF-00-00-12-12
 Platform              : DGS-1520-28MP
 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   DGS-1520-28MP    40    1.01.004
 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   DGS-1520-28MP    40    1.01.004
 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 ***]

MAC Address : 00-02-00-00-08-12
Group Name  : default
Device Name           :
Firmware Version      : 1.01.004
Platform              : DGS-1520-28MP
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#
```

99. Spanning Tree Protocol (STP) Commands

99-1 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#
```

99-2 show spanning-tree

This command is used to display the information of spanning tree protocol operation. This command is only for STP and RSTP.

show spanning-tree [interface [*INTERFACE-ID* **[, | -]]**

Parameters

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

-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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

 Spanning Tree: Enabled
 Protocol Mode: RSTP
 Tx-hold-count: 6
 NNI BPDU Address: dot1d(01-80-C2-00-00-00)
 Root ID Priority: 32768
         Address: F0-7D-68-34-0A-00
         Hello Time: 2 sec, Max Age: 20 sec, Forward Delay: 15 sec
 Bridge  ID Priority: 32768 (priority 32768  sys-id-ext 0)
         Address: F0-7D-68-34-0A-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
 ---------      ----       -----      ----      -------  -----  ----
 eth1/0/1       designated forwarding 200000    128.1    p2p    edge

Switch#
```

99-3 show spanning-tree configuration interface

This command is used to display the information about STP interface related configuration.

show spanning-tree configuration interface [*INTERFACE-ID* **[, | -]]**

Parameters

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

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

Default

None.

Command Mode

User/Privileged EXEC 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 of port 1.

```
Switch#show spanning-tree configuration interface eth1/0/1

eth1/0/1
 Spanning tree state : Enabled
 Port path cost: 0
 Port priority: 128
 Port Identifier:  128.1
 Link type: auto
 Port fast: edge
 Guard root: Disabled
 TCN filter : Disabled
 Bpdu forward: Disabled

Switch#
```

99-4 snmp-server enable traps stp

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

snmp-server enable traps stp [new-root] [topology-chg]

no snmp-server enable traps stp [new-root] [topology-chg]

Parameters

new-root	(Optional) Specifies the sending of STP new root notification.
topology-chg	(Optional) Specifies the sending of STP topology change notification.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the sending of notification traps for STP. If no parameter is specified, both STP notification types are enabled or disabled.

Example

This example shows how to enable the sending of the all traps for STP to the host 10.9.18.100 using the community string defined as public.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps
Switch(config)#snmp-server enable traps stp
Switch(config)#snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

99-5 spanning-tree global state

This command is used to enable the global state of STP. Use the **no** form of this command to disable the state.

spanning-tree global state {enable | disable}

no spanning-tree global state

Parameters

enable	Specifies to enable the STP's global state.
disable	Specifies to disable the STP's global state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable or disable the global state of STP.

Example

This example shows how to enable the STP function.

```
Switch#configure terminal
Switch(config)#spanning-tree global state enable
Switch(config)#
```

99-6 spanning-tree (timers)

This command is used to configure the Spanning Tree timer value. Use the **no** form of this command to revert to the default settings.

spanning-tree {hello-time *SECONDS* **| forward-time** *SECONDS* **| max-age** *SECONDS***}**

no spanning-tree {hello-time | forward-time | max-age}

Parameters

hello-time *SECONDS*	Specifies the interval that a designated port will wait between the periodic transmissions of each configuration message. The range is from 1 to 2 seconds.
forward-time *SECONDS*	Specifies the forward delay time used by STP to transition from the listening to the learning states and learning to forwarding states. The range is from 4 to 30 seconds.
max-age *SECONDS*	Specifies the maximum message age of BPDU. The range is from 6 to 40 seconds.

Default

The default value of the **hello-time** is 2 seconds.

The default value of the **forward-time** is 15 seconds.

The default value of the **max-age** is 20 seconds.

Command Mode

Global Configuration Mode.

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)#
```

99-7 spanning-tree state

This command is used to enable or disable the STP operation. Use the **no** form of this command to revert to the default setting.

spanning-tree state {enable | disable}

no spanning-tree state

Parameters

enable	Specifies to enable STP for the configured interface.
disable	Specifies to disable STP for the configured interface.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree state enable
Switch(config-if)#
```

99-8 spanning-tree cost

This command is used to configure the value of the port path-cost on the specified port. Use the **no** form of this command to 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 on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree cost 20000
Switch(config-if)#
```

99-9 spanning-tree guard root

This command is used to enable the root guard mode. Use the **no** form of this command to revert to the default setting.

spanning-tree guard root

no spanning-tree guard root

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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 port 1 from being a root port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#spanning-tree guard root
Switch(config-if)#
```

99-10 spanning-tree link-type

This command is used to configure a link-type for a port. Use the **no** form of this command to revert to the default setting.

spanning-tree link-type {point-to-point | shared}

no spanning-tree link-type

Parameters

point-to-point	Specifies that the port's link type is point-to-point.
shared	Specifies that the port's link type is a shared media connection.

Default

The link type is automatically derived from the duplex setting unless explicitly configuring the link type.

Command Mode

Interface Configuration Mode.

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 on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree link-type point-to-point
Switch(config-if)#
```

99-11 spanning-tree mode

This command is used to configure the STP mode. Use the **no** form of this command to revert to the default setting.

spanning-tree mode {mstp | rstp |stp}

no spanning-tree mode

Parameters

mstp	Specifies the Multiple Spanning Tree Protocol (MSTP).
rstp	Specifies the Rapid Spanning Tree Protocol (RSTP).
stp	Specifies the Spanning Tree Protocol (IEEE 802.1D Compatible)

Default

By default, this mode is RSTP.

Command Mode

Global Configuration Mode.

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)#
```

99-12 spanning-tree portfast

This command is used to specify the port's fast mode. Use the **no** form of this command to revert to the default setting.

spanning-tree portfast {disable | edge| network}

no spanning-tree portfast

Parameters

disable	Specifies to set the port to the port fast disabled mode.
edge	Specifies to set the port to the port fast edge mode.
network	Specifies to set the port to the port fast network mode.

Default

By default, this option is **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 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)#
```

99-13 spanning-tree port-priority

This command is used to configure the value of the STP port priority on the specified port. It is only used for RSTP and STP versions. Use the **no** form of this command to revert to the default setting.

spanning-tree port-priority *PRIORITY*

no spanning-tree port-priority

Parameters

PRIORITY	Specifies the port priority. Valid values are from 0 to 240.

Default

By default, this value is 128.

Command Mode

Interface Configuration Mode.

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 on port 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree port-priority 0
Switch(config-if)#
```

99-14 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 revert 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 **spanning-tree mst priority** command to configure the priority for an MSTP instance.

Example

This example shows how to configure the STP bridge priority value to 4096.

```
Switch#configure terminal
Switch(config)#spanning-tree priority 4096
Switch(config)#
```

99-15 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 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 7.

```
Switch#configure terminal
Switch(config)#interface eth1/0/7
Switch(config-if)#spanning-tree tcnfilter
Switch(config-if)#
```

99-16 spanning-tree tx-hold-count

This command is used to limit the maximum number of BPDUs that can be sent before pausing for one second. Use the **no** form of this command to revert to the default setting.

spanning-tree tx-hold-count *VALUE*

no spanning-tree tx- hold-count

Parameters

VALUE	Specifies the maximum number of BPDUs that can be sent before pausing for one second. The range is from 1 to 10.

Default

By default, this value is 6.

Command Mode

Global Configuration Mode.

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)#
```

99-17 spanning-tree forward-bpdu

This command is used to enable the forwarding of the spanning tree BPDU. Use the **no** form of this command to disable the forwarding of the spanning tree BPDU.

spanning-tree forward-bpdu

no spanning-tree forward-bpdu

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

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 eth1/0/2
Switch(config-if)#spanning-tree forward-bpdu
Switch(config-if)#
```

99-18 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 this 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)#
```

99-19 spanning-tree loop-guard

This command is used to enable the loop guard mode. Use the **no** form of this command to revert to the default setting.

spanning-tree loop-guard

no spanning-tree loop-guard

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 and port-channel interface configuration.

The STP loop guard feature provides additional protection against Layer 2 forwarding loops (STP loops). An STP loop is created when an STP blocking port in a redundant topology erroneously transitions to the forwarding state. This usually happens because one of the ports of a physically redundant topology (not necessarily the STP blocking port) no longer receives STP BPDUs. In its operation, STP relies on continuous reception or transmission of BPDUs based on the port role. The designated port transmits BPDUs, and the non-designated port receives BPDUs.

When one of the ports in a physically redundant topology no longer receives BPDUs, the STP conceives that the topology is loop free. Eventually, the blocking port from the alternate or backup port becomes designated and moves to a forwarding state. This situation creates a loop.

Example

This example shows how to enable the loop guard mode on port 3.

```
Switch#configure terminal
Switch(config)#interface eth1/0/3
Switch(config-if)#spanning-tree loop-guard
Switch(config-if)#
```

100. Stacking Commands

100-1 stack

This command is used to enable the daisy-chain stacking function. Use the **no** form of this 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 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.

When stacking is enabled, the last 2 or 4 ports are dedicated stacking ports and cannot be used for any other purpose. These ports are only able to perform stacking when stacking is enabled.

Example

This example shows how to enable stacking mode.

```
Switch#stack

 WARNING: The command does not take effect until the next reboot.
Switch#
```

100-2 stack bandwidth

This command is used to change the stacking port bandwidth. Use the **no** form of this command to revert to the default setting.

stack bandwidth {2-port-sfp+ | 2-port-10g-base-t | 4-port-hybrid}

no stack bandwidth

Parameters

2-port-sfp+	Specifies 2 SFP+ switch ports to be used for stacking.

2-port-10g-base-t	Specifies 2 10GBASE-T switch ports to be used for stacking.
4-port-hybrid	Specifies 2 SFP+ and 2 10GBASE-T switch ports to be used for stacking.

Default

By default, 2 SFP+ ports are used.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to change the stacking port bandwidth. The stacking bandwidth must be configured before the Switch is stacked with other switches.

Switches in the series can be physically stacked with optical fiber cables, standard Ethernet cables, or Direct Attached Cables (DACs) with SFP+ connectors. Only the last 4 ports on the Switch can be used for physical stacking.

Stacking ports or grouped together into two logical stacking ports called SIO1 (Stacking Input/Output 1) and SIO2. A group of logical stacking ports must always be connected, as a group, to another Switch in the stack.

The following table lists the stacking configuration with the corresponding SIO port pairs:

Configuration	Switch	Logical SIO1	Logical SIO2	Bandwidth
2-port-10g-base-t	DGS-1520-28	Port 25	Port 26	40 Gbps (full-duplex)
	DGS-1520-28MP	Port 25	Port 26	40 Gbps (full-duplex)
	DGS-1520-52	Port 49	Port 50	40 Gbps (full-duplex)
	DGS-1520-52MP	Port 49	Port 50	40 Gbps (full-duplex)
2-port-sfp+	DGS-1520-28	Port 27	Port 28	40 Gbps (full-duplex)
	DGS-1520-28MP	Port 27	Port 28	40 Gbps (full-duplex)
	DGS-1520-52	Port 51	Port 52	40 Gbps (full-duplex)
	DGS-1520-52MP	Port 51	Port 52	40 Gbps (full-duplex)
4-port-hybrid	DGS-1520-28	Port 25 and 26	Port 27 and 28	80 Gbps (full-duplex)
	DGS-1520-28MP	Port 25 and 26	Port 27 and 28	80 Gbps (full-duplex)
	DGS-1520-52	Port 49 and 50	Port 51 and 52	80 Gbps (full-duplex)
	DGS-1520-52MP	Port 49 and 50	Port 51 and 52	80 Gbps (full-duplex)

Refer to **Appendix G - Stacking Information** for stacking topologies.

Example

This example shows how to change the stacking bandwidth to 4-port.

```
Switch#stack bandwidth 4-port-hybrid

 WARNING: The command does not take effect until the next reboot.
Switch#
```

100-3 stack renumber

This command is used to manually assign a unit ID to a switch unit. Use the **no** form of this 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, 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#
```

100-4 stack priority

This command is used to configure the priority of the switch stacking unit. Use the **no** form of this command to revert to the default setting.

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#
```

100-5 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 this command to disable preemption.

stack preempt

no stack preempt

Parameters

None.

Default

By default, this option is enabled.

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, 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 preempt
Switch#
```

100-6 snmp-server enable traps stack

This command is used to enable the sending of stacking related trap. Use the **no** form of this command to disable the sending of stacking related trap.

snmp-server enable traps stack

no snmp-server enable traps stack

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 or disable the sending of stacking related SNMP notifications.

Example

This example shows how to enable the sending of stacking related trap.

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

Switch(config)#
```

100-7 show stack

This command is used to display the stacking information.

show stack

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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       : Enabled
Trap State          : Disabled

Topology            : Duplex_Ring
My Box ID           : 1
Master ID           : 1
BK Master ID        : 2
Box Count           : 2

Box User Module              Prio-                   Prom      Runtime   H/W
ID  Set  Name          Exist rity  MAC               Version   Version   Version
--- ---- ------------- ----- ----- ----------------- --------- --------- -------
1   Auto DGS-1520-28MP Exist 32    80-26-89-15-28-00 1.00.011  1.01.004 A1
2   Auto DGS-1520-28   Exist 32    80-26-89-15-28-A0 1.00.011  1.01.004 A1
3   -    NOT_EXIST     No
4   -    NOT_EXIST     No
5   -    NOT_EXIST     No
6   -    NOT_EXIST     No
7   -    NOT_EXIST     No
8   -    NOT_EXIST     No

 Stack Bandwidth:
 Box    User Set           SIO1 Active   SIO2 Active
 ID     Bandwidth          Bandwidth     Bandwidth
 ----   ------------------ ---------     ---------
 1      2-port(sfp+)       1-port        1-port
 2      2-port(sfp+)       1-port        1-port
 3
 4
 5
 6
 7
 8

Switch#
```

101. Storm Control Commands

101-1 snmp-server enable traps storm-control

This command is used to enable and configure the sending of SNMP notifications for storm control. Use the **no** form of this command to disable the sending of SNMP notifications.

snmp-server enable traps storm-control [storm-occur] [storm-clear]

no snmp-server enable traps storm-control [storm-occur] [storm-clear]

Parameters

storm-occur	(Optional) Specifies to send a notification when a storm event is detected.
storm-clear	(Optional) Specifies to send a notification when a storm event is cleared.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable the notifications for storm control module. When no optional parameter is specified, both notifications are enabled or disabled. When one of the optional parameters is specified, only the specified notification type is enabled or disabled.

Example

This example shows how to enable the sending of traps for storm control for both storm occurrences and clearances.

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

101-2 storm-control

This command is used to configure the device to protect the device from broadcast, multicast, and DA unknown packet storm attacks. Use the **no** form of this command to revert to the default settings.

storm-control {{broadcast | multicast | unicast} level {pps *PPS-RISE* **[***PPS-LOW***] | kbps** *KBPS-RISE* **[***KBPS-LOW***] |** *LEVEL-RISE* **[***LEVEL-LOW***]} | action {shutdown | drop | none}}**

no storm-control {broadcast | multicast | unicast | action}

Parameters

broadcast	Specifies to set the broadcast rate limit.

multicast	Specifies to set the multicast rate limit.
unicast	Specifies 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 0 to 2147483647. If the low PPS value is not specified, the default value is 80% of the specified risen PPS.
level kbps *KBPS-RISE* **[***KBPS-LOW***]**	Specifies the threshold value as a rate of bits per second at which traffic is received on the port. The range is from 0 to 2147483647. If the low KBPS is not specified, the default value is 80% of the specified risen KBPS.
level *LEVEL-RISE* **[***LEVEL-LOW***]**	Specifies the threshold value as a percentage of the total bandwidth per port at which traffic is received on the port. The range is from 0 to 100. If the low level is not specified, the default value is 80% of the specified risen level.
action shutdown	Specifies to shut down the port when the value specified for rise threshold is reached.
action drop	Specifies to discards packets that exceed the risen threshold.
action none	Specifies not to filter the storm packets.

Default

By default, the broadcast, multicast, and unicast (DLF) storm controls are disabled.

The default action taken when a storm occurs is to drop storm packets.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

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.

The threshold can be specified as percentage of port bandwidth, kilobytes per second or as packet count per second.

It is unable to give the precise suppression level for percentage (0 to 100) of total bandwidth of specific port interface. The current calculation formula assumes that the packet size is 64 bytes.

If the storm control action is set to drop, the packet will be dropped when the traffic rate exceeds the threshold level.

If the action is set to shutdown, the port will enter the error disabled state when the traffic load of the monitored flooding packet exceeds the rising threshold.

Example

This example shows how to enable broadcast storm control on ports 1 and 2. It sets the threshold of port 1 to 500 packets per second with the shutdown action and sets the threshold of port 2 between 60% and 70% with the drop action.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#storm-control broadcast level pps 500
Switch(config-if)#storm-control action shutdown
Switch(config-if)#exit
Switch(config)#interface eth1/0/2
Switch(config-if)#storm-control broadcast level 70 60
Switch(config-if)#storm-control action drop
Switch(config-if)#
```

101-3 storm-control polling

This command is used to configure the polling interval of received packet counts. Use the **no** form of this command to revert to the default settings.

storm-control polling {interval *SECONDS* **| retries {***NUMBER* **| infinite}}**

no storm-control polling {interval | retries}

Parameters

interval *SECONDS*	Specifies the polling interval of received packet counts. This value must be between 5 and 600 seconds.
retries *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)#
```

101-4 show storm-control

This command is used to display the current storm control settings.

show storm-control interface *INTERFACE-ID* **[, | -] [broadcast | multicast | unicast]**

Parameters

interface *INTERFACE-ID*	Specifies the port's interface ID.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
broadcast	(Optional) Specifies to display the current broadcast storm setting.
multicast	(Optional) Specifies to display the current multicast storm setting.
unicast	(Optional) Specifies to display the current unicast (DLF) storm setting.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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 on ports 1 to 6.

```
Switch#show storm-control interface eth1/0/1-6 broadcast

Interface    Action    Threshold         Current    State
-------------------------------------------------------
eth1/0/1     Drop      500/300 pps       200 pps    Forwarding
eth1/0/2     Drop      80/64 %           20 %       Forwarding
eth1/0/3     Drop      80/64 %           70 %       Dropped
eth1/0/4     Shutdown  60/50 %           20 %       Forwarding
eth1/0/5     None      60000/50000 kbps  2000 kbps  Forwarding
eth1/0/6     None      -                 -          Inactive

Total Entries: 6

Switch#
```

This example shows how to display all types of storm control settings on ports 1 to 2.

```
Switch#show storm-control interface eth1/0/1-2

Polling Interval       : 15 sec           Shutdown Retries       : Infinite
Trap                   : Disabled
Interface      Storm         Action      Threshold     Current    State
---------------------- ------------------------------------------
eth1/0/1       Broadcast     Drop        80/64 %       50%        Forwarding
eth1/0/1       Multicast     Drop        80/64 %       50%        Forwarding
eth1/0/1       Unicast       Drop        80/64 %       50%        Forwarding
eth1/0/2       Broadcast     Shutdown    500/300 pps   -          Error Disabled
eth1/0/2       Multicast     Shutdown    500/300 pps   -          Error Disabled
eth1/0/2       Unicast       Shutdown    500/300 pps   -          Error Disabled

Total Entries: 6

Switch#
```

Display Parameters

Interface	The interface ID.
Action	The configured action, the possible actions are: Drop, Shutdown, None.
Threshold	The configured threshold.
Current	The actual traffic rate which is currently flowing though the interface. Its unit may be percentage, kbps, PPS based on the configured meter mode. Because hardware can only counts by PPS, this value of this filed may be a rough value for percentage and kbps.
State	The current state of storm control on a given interface for a given traffic type. The possible states are: **Forwarding:** No storm event has been detected. **Dropped:** A storm event has occurred and the storm traffic exceeding the threshold is dropped. **Error Disabled:** The port is disabled due to a storm. **Link Down:** The port is physically linked down. **Inactive:** Indicates that storm control is not enabled for the given traffic type.

102. Super VLAN Commands

102-1 supervlan

This command is used to configure the VLAN as a super VLAN. Use the **no** form of this 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 and proxy ND 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)#
```

102-2 subvlan

This command is used to add sub-VLANs to a super VLAN. Use the **no** form of this 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 separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

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

 WARNING: Proxy ARP will be enabled automatically on this super VLAN.

Switch(config-vlan)#subvlan 5-7
Switch(config-vlan)#
```

102-3 subvlan-address-range

This command is used to configure the IP address range of a sub-VLAN. Use the **no** form of this 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)#
```

102-4 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 be displayed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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           Inactive        192.168.10.1 - 192.168.10.50
               6           Inactive
               7           Inactive

Switch#
```

103. Surveillance VLAN Commands

103-1 surveillance vlan

This command is used to enable the global surveillance VLAN state and configure the surveillance VLAN. Use the **no** form of this command to disable the surveillance VLAN state.

surveillance vlan *VLAN-ID*

no surveillance vlan

Parameters

VLAN-ID	Specifies the ID of the surveillance VLAN. The range is from 2 to 4094.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the global surveillance VLAN function and to specify the surveillance VLAN on the Switch. Each switch can only have one Surveillance VLAN.

Both the **surveillance vlan** command in Global Configuration Mode and the **surveillance vlan enable** command in Interface Configuration Mode need to be enabled for a port to start the surveillance VLAN function.

When the surveillance VLAN is enabled for a port, the port will be automatically learned as surveillance VLAN untagged member, the received untagged surveillance packets will be forwarded to the surveillance VLAN. The received packets are determined as surveillance packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **surveillance vlan mac-address** command.

A VLAN needs to be created before assigning the VLAN as the surveillance VLAN.

If the surveillance VLAN is configured, this VLAN cannot be removed using the **no vlan** command.

Example

This example shows how to enable the surveillance VLAN function and configure VLAN 1001 as a Surveillance VLAN.

```
Switch#configure terminal
Switch(config)#surveillance vlan 1001
Switch(config)#
```

103-2 surveillance vlan aging

This command is used to configure the aging time for aging out the surveillance VLAN dynamic member ports Use the **no** form of this command to revert to the default setting.

surveillance vlan aging *MINUTES*

no surveillance vlan aging

Parameters

MINUTES	Specifies the aging time of surveillance VLAN. The range is from 1 to 65535 minutes.

Default

By default, this aging time is 720 minutes.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the aging time for aging out the surveillance device and the surveillance VLAN automatically learned member ports.

When the last surveillance device connected to the port stops sending traffic, and the MAC address of this surveillance device is aged out, the surveillance VLAN aging timer will be started. The port will be removed from the surveillance VLAN after expiration of surveillance VLAN aging timer.

If the surveillance traffic resumes during the aging time, the aging timer will be cancelled.

Example

This example shows how to configure the aging time of surveillance VLAN to 30 minutes.

```
Switch#configure terminal
Switch(config)#surveillance vlan aging 30
Switch(config)#
```

103-3 surveillance vlan enable

This command is used to enable the surveillance VLAN state of ports. Use the **no** form of this command to disable the surveillance vlan state of ports.

surveillance vlan enable

no surveillance vlan enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

The command takes effect for access ports or hybrid ports.

Use this command to enable the surveillance VLAN function for ports.

Both the **surveillance vlan** command in Global Configuration Mode and the **surveillance vlan enable** command in Interface Configuration Mode need to be enabled for a port to start the surveillance VLAN function.

When surveillance VLAN is enabled for a port, the port will be automatically learned as surveillance VLAN untagged member, the received untagged surveillance packets will be forwarded to surveillance VLAN. The received packets are determined as surveillance packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **surveillance vlan mac-address** command.

Example

This example shows how to enable surveillance VLAN function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#surveillance vlan enable
Switch(config-if)#
```

103-4 surveillance vlan mac-address

This command is used to add the user-defined surveillance device OUI. Use the **no** form of this command to delete the user-defined surveillance device OUI.

surveillance vlan mac-address *MAC-ADDRESS MASK* **[component-type {vms | vms-client | video-encoder | network-storage | other} description** *TEXT***]**

no surveillance vlan mac-address *MAC-ADDRESS MASK*

Parameters

MAC-ADDRESS	Specifies the OUI MAC address.
MASK	Specifies the OUI MAC address matching bitmask.
component-type	(Optional) Specifies surveillance components that could be auto-detected by surveillance VLAN.
vms	(Optional) Specifies the surveillance components type as Video Management Server (VMS).
vms-client	(Optional) Specifies the surveillance components type as VMS client.
video-encoder	(Optional) Specifies the surveillance components type as Video Encoder.
network-storage	(Optional) Specifies the surveillance components type as Network Storage.
other	(Optional) Specifies the surveillance components type as other IP Surveillance Devices.
description *TEXT*	(Optional) Specifies the description for the user-defined OUI with a maximum of 32 characters.

Default

OUI Address	Mask	Component Type	Description
28-10-7B-00-00-00	FF-FF-FF-E0-00-00	D-Link Device	IP Surveillance Device
28-10-7B-20-00-00	FF-FF-FF-F0-00-00	D-Link Device	IP Surveillance Device

B0-C5-54-00-00-00	FF-FF-FF-80-00-00	D-Link Device	IP Surveillance Device
F0-7D-68-00-00-00	FF-FF-FF-F0-00-00	D-Link Device	IP Surveillance Device

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to add user-defined OUI(s) for the surveillance VLAN. The OUI for surveillance VLAN are used to identify the surveillance traffic by the surveillance VLAN function.

If the source MAC addresses of the received packet matches any of the OUI pattern, the received packet is determined as a surveillance packet.

The user-defined OUI cannot be the same as the default OUI.

The default OUI cannot be deleted.

Example

This example shows how to add a user-defined OUI for surveillance devices.

```
Switch#configure terminal
Switch(config)#surveillance vlan mac-address 00-01-02-03-00-00 FF-FF-FF-FF-00-00 component-type vms description user1
Switch(config)#
```

103-5 surveillance vlan qos

This command is used to configure the CoS priority for the incoming surveillance VLAN traffic. Use the **no** form of this command to revert to the default setting.

surveillance vlan qos *COS-VALUE*

no surveillance vlan qos

Parameters

COS-VALUE	Specifies the priority of surveillance VLAN. The available value is from 0 to 7.

Default

The default value 5.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The surveillance packets arriving at the surveillance VLAN enabled port are marked to the COS specified by the command. The remarking of COS allows the surveillance VLAN traffic to be distinguished from data traffic in quality of service.

Example

This example shows how to configure the priority of the surveillance VLAN to be 7.

```
Switch#configure terminal
Switch(config)#surveillance vlan qos 7
Switch(config)#
```

103-6 show surveillance vlan

This command is used to display the surveillance VLAN configurations.

show surveillance vlan [interface [*INTERFACE-ID* **[, | -]]]**

show surveillance vlan device [interface [*INTERFACE-ID* **[, | -]]]**

Parameters

device	Specifies to display the learned surveillance devices information.
interface	(Optional) Specifies to display surveillance VLAN information of ports.
INTERFACE-ID	(Optional) Specifies the port to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the surveillance VLAN configurations.

The **show surveillance vlan** command is used to display the surveillance VLAN global configurations. The **show surveillance vlan interface** command is used to display the surveillance VLAN configurations on the interfaces. The **show surveillance vlan device** command is used to display the surveillance device discovered by its OUI.

Example

This example shows how to display the surveillance VLAN global settings.

```
Switch#show surveillance vlan

 Surveillance VLAN ID  : 1001
 Surveillance VLAN CoS : 5
 Aging Time            : 30 minutes
 Member Ports          :
 Dynamic Member Ports  :

 Surveillance VLAN OUI :

 OUI Address        Mask               Component Type   Description
 -----------------  -----------------  ---------------  --------------
 28-10-7B-00-00-00  FF-FF-FF-E0-00-00  D-Link Device    IP Surveillance Device
 28-10-7B-20-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device
 B0-C5-54-00-00-00  FF-FF-FF-80-00-00  D-Link Device    IP Surveillance Device
 F0-7D-68-00-00-00  FF-FF-FF-F0-00-00  D-Link Device    IP Surveillance Device

 Total OUI: 4

Switch#
```

This example shows how to display the learned surveillance device on ports 1 and 2.

```
Switch#show surveillance vlan device interface eth1/0/1-2

                                              Component Type/
 Interface       Device             Start Time  Description
 --------------  -----------------  ----------  ---------------
 eth1/0/1        00-01-02-03-00-01  2011-10-06  VMS
                                    09:00       IP Surveillance Device
 eth1/0/2        00-01-02-03-00-02  2011-10-06  VMS
                                    14:10       IP Surveillance Device
 eth1/0/2        F0-7D-68-03-44-A1  2011-10-06  D-Link Device
                                    17:15       user1

 Total Entries : 3

Switch#
```

104. Switch Port Commands

104-1 duplex

This command is used to configure the physical port interface's duplex setting. Use the **no** form of this command to revert to the default settings.

duplex {full | half | auto}

no duplex

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.

Default

The duplex mode is set as **auto** for 100BASE-T, 2500BASE-T, and 10GBASE-T interfaces.

The duplex mode is fixed to **full** for 10GBASE-R interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

For the 2500BASE-T and 10GBASE-T module, the duplex mode cannot be set to half.

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, 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, the advertised capability will be both full and half duplex modes combined with the configured speeds.

Example

This example shows how to configure port 1 to operate at a forced speed of 100Mbits and specifies that the duplex mode should be set to auto-negotiated.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#speed 100
Switch(config-if)#duplex auto
Switch(config-if)#
```

104-2 flowcontrol

This command is used to configure the flow control capability of the port interface. Use the **no** form of this 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.

This command does not work through Switches that are physically stacked.

Example

This example shows how to enable the flow control on port 1.

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

104-3 mdix

This command is used to configure the port Media-Dependent Interface Crossover (MDIX) state. Use the **no** form of this 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 auto on port 1.

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

104-4 speed

This command is used to configure the physical port interface's speed settings. Use the **no** form of this command to revert to the default setting.

NOTE: 10G does not support speed configurations of 10Mbps, 100Mbps, and 2.5Gbps.

speed {10 | 100 | 1000 [master | slave] | 2500 [master | slave] | 10giga [master | slave] | auto [*SPEED-LIST***]}**

no speed

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.
2500	Specifies to force the speed to 2.5Gbps.
master | slave	Specifies the port operates as master or slave timing. This parameter is only applicable to 1000BASE-T or 2500BASE-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.

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, 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 **10**, **100**, **1000**, **2500**, and/or **10giga**. If the speed list is not specified, all speed will be advertised. Use the hyphen symbol to separate a range of values or use the comma symbol to separate a series of values. No space is allowed before or after the symbols.

Default

The speed is set as **auto** for 100BASE-T, 2500BASE-T and 10GBASE-T interfaces.

The speed is fixed to 10Gbps for 10GBASE-R interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

If the specified speed is not supported by the hardware, error messages will be returned.

For the 1000BASE-T connection, when the speed is set as 1000, the port must be configured as master or slave.

For the 2500BASE-T connection, when the speed is set as 1000 or 2500, the port must be configured as master or slave.

For the 10GBASE-T connection, when the speed is set as 1000 or 10giga, the port must be configured as master or slave.

When the speed is set as 10giga, the duplex mode cannot be set as half, and vice versa.

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, 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**, the advertised capability will be both half and full duplex modes combined with the specified speeds.

Example

This example shows how to configure port 1 to only auto-negotiate to 10Mbps or 100Mbps.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#speed auto 10,100
Switch(config-if)#
```

105. System File Management Commands

105-1 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)#
```

105-2 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] [all] *URL*

Parameters

check	(Optional) Specifies to display the firmware information for the specified file. This information includes the version number and model description.
all	(Optional) Specifies to apply the boot image file to all switch units in stack.
URL	Specifies the URL of the file to be used as the boot image file.

Default

By default, there is one image file as the boot image.

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: 1.01.004
Description: D-Link Corporation Gigabit Ethernet Smart Managed 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)#
```

105-3 clear running-config

This command is used to clear the system’s running configuration.

clear running-config

Parameters

None.

Default

None.

Command Mode

Privileged 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 the system's configuration to the factory
default settings, including the IP address.
Clear running configuration? (y/n) [n] y

Switch#
```

105-4 reset system

This command is used to reset the system, clear the system's configuration, and then save and reboot the Switch.

reset system

Parameters

None.

Default

None.

Command Mode

Privileged 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 the system's configuration to the factory
default settings, including the IP address and stacking settings.
Clear system configuration, save, reboot? (y/n) [n] y
Saving configurations and logs to NV-RAM......   Done
Please wait, the switch is rebooting...
```

105-5 configure replace

This command is used to replace the current running configuration with the indicated configuration file.

configure replace {{tftp: *//LOCATIONIFILENAME* **| sftp:** *//LOCATIONIFILENAME***} | flash:** *FILENAME***} [force]**

Parameters

tftp:	Specifies that the configuration file is from the TFTP server.
//LOCATIONIFILENAME	Specifies the URL of the configuration file on the TFTP server.
sftp:	Specifies that the configuration file is from the SFTP server. The SFTP client settings must be configured before using this parameter.
//LOCATIONIFILENAME	Specifies the URL of the configuration file on the SFTP server.
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

Privileged 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 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#
```

105-6 copy

This command is used to copy a file to another file.

copy *SOURCE-URL DESTINATION-URL*

copy *SOURCE-URL* **{tftp: [***IILOCATIONIDESTINATION-URL***] | sftp: [***IILOCATIONIDESTINATION-URL***]}**

copy {tftp: [*IILOCATIONISOURCE-URL***] | sftp: [***IILOCATIONISOURCE-URL***]}** *DESTINATION-URL*

Parameters

SOURCE-URL	Specifies the source URL for the source file to be copied. One special form of the URL is represented by the following keywords. If **startup-config** is specified as the *SOURCE-URL*, the purpose is to upload the startup configuration, save the startup configuration as the file in the file system, or to execute the startup configuration as the running configuration. If **running-config** is specified as the *SOURCE-URL*, the purpose is to upload the running configuration or save the running configuration as the startup configuration or to save it as the file in the file system.

	If **flash: [***PATH-FILE-NAME***]** is specified as the *SOURCE-URL*, the purpose is to specify the source file to be copied in the file system. If **log** is specified as the *SOURCE-URL*, the system log can be retrieved to the TFTP server 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	(Optional) Specifies the IPv4 address of the TFTP/SFTP server or IPv6 address of the TFTP server.

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 or SFTP 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 or SFTP server, the URL must be prefixed with “tftp: //” or “sftp: //”.

To download the firmware image, the user should use the **copy tftp: //** or **copy sftp: //** command to download the file from the TFTP or SFTP 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 15710864 bytes.
 Transmission to slave start.................. Done.
 Transmission to slave finished, file length 15710864 bytes.
 Please wait, programming flash.............. 100 %
 Please wait, programming flash for language files .............Done.
 Wait slave programming flash complete...
 Done.

Switch#
```

This example shows how to upload the running configuration to the SFTP server and replace the current running configuration.

```
Switch#configure replace sftp: //10.90.90.23/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

Address of remote host [10.90.90.23]?
Source filename [config.cfg]?
Destination filename [config.cfg]?
 Start, aborted by CTRL+C or Esc, remote_file_path is config.cfg
 Connecting to remote server 10.90.90.23
 Server's host key fingerprint (MD5):
 89:40:F4:5D:70:8B:97:13:44:D4:F2:79:1B:4E:EF:AB
 Unknown server, Are you sure you want to continue connecting (y/n)?:y
 User Name [Anonymous]:admin
 Password:****
 Download ................ 100 %
 Please wait, programming flash.............. Done.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to download an image file from the SFTP server to all units in the stack.

```
Switch#copy sftp: //10.90.90.23/sftpfile.had flash: sftpfile.had

Address of remote host [10.90.90.23]?
Source filename [sftpfile.had]?
Destination filename [sftpfile.had]?
 Start, aborted by CTRL+C or Esc, remote_file_path is sftpfile.had
 Connecting to remote server 10.90.90.23
 Server's host key fingerprint (MD5):
 89:40:F4:5D:70:8B:97:13:44:D4:F2:79:1B:4E:EF:AB
 Unknown server, Are you sure you want to continue connecting (y/n)?:y
 User Name [Anonymous]:admin
 Password:****
 Download ................ 100 %
 Please wait, programming flash.............. Done.
 Please wait, programming flash for language files .............Done.
 Wait slave programming flash complete...
 Done.

Switch#
```

105-7 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. Use the **no** form of this command to revert to the default setting.

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.

This command is only available for Loopback, MGMT (DGS-1520-28 and DGS-1520-52 Only), and VLAN interface configuration.

Example

This example shows how to download software from VLAN 1.

```
Switch#configure terminal
Switch(config)#ip tftp source-interface vlan 1
Switch(config)#
```

105-8 reboot

This command is used to reboot the Switch.

reboot [force_agree]

Parameters

force_agree	(Optional) Specifies to restart the Switch without confirmation.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to reboot the Switch.

Example

This example shows how to reboot the Switch.

```
Switch# reboot force_agree

Please wait, the switch is rebooting...
```

105-9 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/Privileged EXEC 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:/config.cfg


Switch#
```

105-10 show running-config

This command is used to display the commands in the running configuration file.

show running-config [effective | all] [interface *INTERFACE-ID* **| vlan** *VLAN-ID***]**

Parameters

effective	(Optional) Specifies to display command configurations that 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*	(Optional) Specifies to display command configurations corresponding to the specified interface.
vlan *VLAN-ID*	(Optional) Specifies to display command configurations corresponding to the specified VLAN.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command displays the current running system configuration. If no parameter is specified, only the modified configuration part, other than the default configuration, will be displayed.

Example

This example shows how to display the content of the running configuration file.

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

Current configuration : 1891 bytes

!----------------------------------------------------------------------------
!                 DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                               Configuration
!
!                            Firmware: Build 1.01.004
!           Copyright(C) 2022 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

stack
!
ip http timeout-policy idle 36000
ignore wizard
!
line console
 session-timeout 0
!
line telnet
!
line ssh
!
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

105-11 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

Privileged EXEC 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

!----------------------------------------------------------------------------
!                 DGS-1520-28MP Gigabit Ethernet Smart Managed Switch
!                               Configuration
!
!                           Firmware: Build 1.01.004
!           Copyright(C) 2022 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
!
ip http timeout-policy idle 36000
ignore wizard
!
# LOGIN START
line console
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

106. System Log Commands

106-1 clear logging

This command is used to delete log messages in the system logging buffer.

clear logging

Parameters

None.

Default

None.

Command Mode

Privileged 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#
```

106-2 logging on

This command is used to enable the logging of system messages. Use the **no** form of this command to disable the logging of system messages.

logging on

no logging on

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

To enable the logging of system messages, use the **logging on** command in the Global Configuration Mode. This command sends debug or error messages to a logging process, which logs messages to designated locations asynchronously to the processes that generated the messages. To disable the logging process, use the **no** form of this command.

The logging process controls the distribution of logging messages to the various destinations, such as the logging buffer, terminal lines, or the syslog server. System logging messages are also known as system error messages. Logging can be turned on and off for these destinations individually using the **logging buffered**, **logging server**, and logging global configuration commands. However, if the **logging on** command is disabled, no messages will be sent to these destinations. If the **logging on** command is enabled, the logging buffered will be enabled at the same time.

Example

This example shows how to enable the logging of system messages.

```
Switch#configure terminal
Switch(config)#logging on
WARNING: The command takes effect and the logging buffered is enabled at the same time.
Switch(config)#
```

106-3 logging buffered

This command is used to enable logging of system messages to the local message buffer. Use the **no** form of this command to disable the logging of messages to the local message buffer. Use the **default logging buffered** command to revert to default setting.

logging buffered [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***] [write-delay {***SECONDS* **| infinite}]**

no logging buffered

default logging buffered

Parameters

SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If this parameter is not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Optional) Specifies to filter the message to be sent to local buffer based on the discriminator.
write-delay *SECONDS*	(Optional) Specifies to delay periodical writing of the logging buffer to the flash memory by the amount of seconds specified. If this parameter is not specified, the default value is 300 seconds.

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)#
```

106-4 logging console

This command is used to enable the logging of system messages to the local console. Use the **no** form of this command to disable the logging of messages to the local console and revert to the default setting.

logging console [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

no logging console

Parameters

SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If this parameter is not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).

discriminator	(Optional) Specifies to filter the message to be sent to the local console based on the discriminator.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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)#
```

106-5 logging monitor

This command is used to enable the logging of system messages to terminals such as Telnet and SSH. Use the **no** form of this command to disable the function.

logging monitor [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

no logging monitor

Parameters

SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If this parameter is not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator	(Optional) Specifies to filter the message to be sent to local buffer 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 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 to the terminal. The messages which are at the specified severity level or higher will be logged to the terminal.

Example

This example shows how to enable the logging of messages to the terminal and restrict logging of messages with a security level of errors or higher.

```
Switch#configure terminal
Switch(config)#logging monitor severity errors
Switch(config)#
```

106-6 logging discriminator

This command is used to create a discriminator that can be further used to filter SYSLOG messages sent to various destinations. Use the **no** form of this command to remove the discriminator.

logging discriminator *NAME* **[facility {drops** *STRING* **| includes** *STRING***}] [severity {drops** *SEVERITY-LIST* **| includes** *SEVERITY-LIST***}]**

no 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)#
```

106-7 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***} [severity {***SEVERITY-LEVEL* | *SEVERITY-NAME***}] [facility {***FACILITY-NUM* | *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

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

Parameters

IP-ADDRESS	Specifies the IP address of the SYSLOG server host.
IPV6-ADDRESS	Specifies the IPv6 address of the log server host.
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If this parameter is not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
FACILITY-NUM	(Optional) Specifies a decimal value from 0 to 23 to represent the facility. If this parameter is not specified, the default facility is local7 (**23**). See the usage guideline for more information.
FACILITY-NAME	(Optional) Specifies a facility name to represent the facility. If this parameter is not specified, the default facility is **local7** (23). See the usage guideline for more information.
discriminator *NAME*	(Optional) Specifies to filter the message to the log server based on discriminator.

port *UDP-PORT*	(Optional) Specifies the UDP port number to be used for the SYSLOG server. Valid values are 514 (the IANA well-known port) or any value from 1024 to 65535. If this parameter is 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.

Facility Number	Facility Name	Facility Description
0	kern	Kernel messages.
1	user	User-level messages.
2	mail	Mail system.
3	daemon	System daemons.
4	auth1	Security/authorization messages.
5	syslog	Messages generated internally by the SYSLOG.
6	lpr	Line printer sub-system.
7	news	Network news sub-system.
8	uucp	UUCP sub-system.
9	clock1	Clock daemon.
10	auth2	Security/authorization messages.
11	ftp	FTP daemon.
12	ntp	NTP subsystem.
13	logaudit	Log audit.
14	logalert	Log alert.
15	clock2	Clock daemon (note 2).
16	local0	Local use 0 (local0).
17	local1	Local use 1 (local1).
18	local2	Local use 2 (local2).
19	local3	Local use 3 (local3).
20	local4	Local use 4 (local4).
21	local5	Local use 5 (local5).
22	local6	Local use 6 (local6).
23	local7	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)#
```

106-8 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 message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If this parameter is not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).
discriminator *NAME*	(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)#
```

106-9 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. Use the **no** form of this command to revert to the default setting.

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.

Only Loopback, MGMT and VLAN interfaces are supported in this command.

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)#
```

106-10 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	(Optional) Specifies to display all log entries starting from the latest message.
REF-SEQ	(Optional) Specifies to start the display from the reference sequence number.
+ *NN*	(Optional) 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*	(Optional) 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/Privileged EXEC 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 2015-03-25 16:37:36 Unit 1, Successful login through Console (Username: Anonymous)
#1 2015-03-25 16:35:54 INFO(6) Port eth1/0/1 link up, 1000Mbps FULL duplex

Switch#
```

106-11 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 *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/Privileged EXEC 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  2015-03-24 15:00:14 CRIT(2) Land attack is blocked from (IP: 10.72.24.1 Port: 7)
Switch#
```

106-12 clear attack-logging

This command is used to delete the attack log.

clear attack-logging {unit *UNIT-ID* **| all}**

Parameters

unit *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

Privileged 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#
```

107. Time and SNTP Commands

107-1 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

Privileged 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 no need to set the software clock. Use this command if no other time sources are available. The time specified in this command is assumed to be in the time zone specified by the configuration of the **clock timezone** command. The clock configured by this command will be applied to RTC if it is available. The configured clock will not be stored in the configuration file.

If the clock is manually set and the SNTP server is configured, the system will still try to sync the clock with the server. If the clock is manually set, but a new clock time is obtained by the SNTP server, the clock will be replaced by the new synced clock.

Example

This example shows how to manually set the software clock to 6:00 p.m. on Jul. 4, 2013.

```
Switch#clock set 18:00:00 4 Jul 2013
Switch#
```

107-2 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 start and end month (by name, January, Jan, February, Feb, 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 apr 2:00 last sun oct 2:00
Switch(config)#
```

107-3 clock timezone

This command is used to set the time zone for display purposes. Use the **no** form of this command to set the time to the Coordinated Universal Time (UTC).

clock timezone {+ | -} *HOURS-OFFSET* **[***MINUTES-OFFSET***]**

no clock timezone

Parameters

+	Specifies that time to be added to UTC.
-	Specifies that time to be subtracted from UTC.
HOURS-OFFSET	Specifies the difference in hours from UTC.
MINUTES-OFFSET	(Optional) Specifies the difference in minutes 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 behind of UTC.

```
Switch#configure terminal
Switch(config)#clock timezone - 8
Switch(config)#
```

107-4 show clock

This command is used to display the time and date information.

show clock

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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    : System Clock
     Current Time           : 00:02:17, 2019-01-01
     Time Zone              : UTC +00:00
     Daylight Saving Time   : Disabled

Switch#
```

107-5 show sntp

This command is used to display information about the SNTP server.

show sntp

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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 Poll Interval        : 720 sec

SNTP Server Status:

SNTP Server                                    Version Last Receive
---------------------------------------------- ------- ---------------
10.0.0.11                                      4       00:02:02
10::2                                          ------- ---------------
FE80::1111%vlan1                               ------- ---------------
---------------------------------------------- ------- ---------------

Total Entries:3

Switch#
```

107-6 sntp server

This command is used to allow the system clock to be synchronized with an SNTP time server. Use the **no** form of this command to remove a server from the list of SNTP servers.

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

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

Parameters

IP-ADDRESS	Specifies the IP address of the time server which provides the clock synchronization.
IPV6-ADDRESS	Specifies the IPv6 address of the time server.

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. 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)#
```

107-7 sntp enable

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

sntp enable

no sntp enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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)#
```

107-8 sntp interval

This command is used to set the interval for the SNTP client to synchronize its clock with the server. Use the **no** form of this command to revert to the default setting.

sntp interval *SECONDS*

no sntp interval

Parameters

SECONDS	Specifies the synchronization interval from 30 to 99999 seconds.

Default

By default, this value is 720 seconds.

Command Mode

Global Configuration Mode.

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)#
```

108. Time Range Commands

108-1 periodic

This command is used to specify the period of time for a time range profile. Use the **no** form of this command to remove the specified period of time.

periodic {daily *HH:MM* **to** *HH:MM* **| weekly** *WEEKLY-DAY HH:MM* **to [***WEEKLY-DAY***]** *HH:MM***}**

no periodic {daily *HH*:*MM* **to** *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)#
```

108-2 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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no optional parameter is specified, all configured time-range profiles will be displayed.

Example

This example shows how to display all the configured time ranges.

```
Switch#show time-range

Time Range Profile: rdtime
Daily 09:00 to 12:00
Weekly Saturday   00:00 to Monday     00:00

Total Entries: 1

Switch#
```

108-3 time-range

This command is used to enter the Time-range Configuration Mode to define a time range. Use the **no** form of this command to delete a time range.

time-range *NAME*

no time-range *NAME*

Parameters

NAME	Specifies the name of the time-range profile to be configured. The maximum length is 32 characters.

Default

None.

Command Mode

Global Configuration Mode.

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 and will not be displayed when issuing the **show time-range** command.

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)#
```

109. Traffic Segmentation Commands

109-1 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 the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

If no parameter is specified, the traffic segmentation configuration for all ports will be displayed.

Example

This example shows how to display the configuration of traffic segmentation on port 1.

```
Switch#show traffic-segmentation forward interface eth1/0/1

Interface        Forwarding Domain
--------------   ----------------------------------------------------------------
eth1/0/1         eth1/0/3-1/0/6

Total Entries: 1

Switch#
```

109-2 traffic-segmentation forward

This command is used to restrict the Layer 2 packet forwarding domain of packets received by the configured port. Use the **no** form of this command to remove the specification of forwarding domain.

traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

no traffic-segmentation forward interface *INTERFACE-ID* **[, | -]**

Parameters

INTERFACE-ID	Specifies the interfaces to be used. The allowed interfaces include physical port.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

Interface Configuration Mode.

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 of this command to remove the specified interface from the traffic segmentation forward member list.

The traffic segmentation member list can be comprised of different interface types, for example port and port-channel in the same forwarding domain. If the interfaces specified by the command include a port-channel, all the member ports of this port-channel will be included in the forwarding domain.

If the forwarding domain of an interface is empty, there is no restriction on Layer 2 forwarding of packets received by the port.

Example

This example shows how to configure traffic segmentation. It restricts the flooding domain of port 1 to the range of ports 3 to 6.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#traffic-segmentation forward interface eth1/0/3-6
Switch(config-if)#
```

110. Transport Layer Security (TLS) Commands

110-1 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: 15.

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 trustpoint. 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 trustpoint *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)#
```

110-2 crypto pki import pem

This command is used to import the CA certificate or the Switch certificate and keys to a trustpoint 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 trustpoint that is associated with the imported certificates and key pairs.
FILE-SYSTEM	Specifies the file system for certificates and key pairs. A colon (:) is required after the specified file system. For example, “flash:” represents the local flash.
DIRECTORY	(Optional) Specifies the directory name where the Switch should import the certificates and key pairs in the Switch or TFTP server.
FILE-NAME	Specifies the name of the certificates and key pairs to be imported. By default, the Switch will append this name with *.ca*, *.prv* and *.crt* for CA certificate, private key and certificate respectively.
password *PASSWORD-PHRASE*	(Optional) Specifies the encrypted password phrase that is used to undo encryption when the private keys are imported. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
tftp	Specifies the source URL for a TFTP network server.
IP-ADDRESS	Specifies the IP address of the TFTP server.
ca	Specifies to import the CA certificate only.
local	Specifies to import local certificate and key pairs only.
both	Specifies to import the CA certificate, local certificate and key pairs.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

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 trustpoint 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 trustpoint does not exist, an error message will be prompted.

Example

This example shows how to import certificates (CA and local) and key pair files to trustpoint "TP1" via TFTP.

```
Switch#configure terminal
Switch(config)#crypto pki import TP1 pem tftp: //10.1.1.2/name/msca password abcd1234 both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via eth1/0/5):!
[OK - 1082 bytes]

% Importing private key PEM file...
Reading file from tftp://10.1.1.2/name/msca.prv
Loading name/msca.prv from 10.1.1.2 (via eth1/0/5):!
[OK - 573 bytes]

% Importing certificate PEM file...
Reading file from tftp://10.1.1.2/name/msca.crt
Loading name/msca.crt from 10.1.1.2 (via eth1/0/5):!
[OK - 1289 bytes]
% PEM files import succeeded.

Switch(config)#
```

110-3 crypto pki trustpoint

This command is used to declare the trustpoint that the Switch will use. Use the **no** form of this command to delete all certificates and key pairs associated with the trustpoint.

crypto pki trustpoint *NAME*

no crypto pki trustpoint *NAME*

Parameters

NAME	Specifies to create a name for the trustpoint.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to declare a trustpoint, 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 trustpoint "TP1" and specify it is a primary trustpoint.

```
Switch#configure terminal
Switch(config)#crypto pki trustpoint TP1
Switch(ca-trustpoint)#primary
Switch(ca-trustpoint)#
```

110-4 crypto pki certificate chain

This command is used to enter the Certificate Chain Configuration Mode.

crypto pki certificate chain *NAME*

Parameters

NAME	Specifies the name for the trustpoint.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to enter the Certificate Chain Configuration Mode. If the specified trustpoint name does not exist, an error message will be displayed.

Example

This example shows how to enter he Certificate Chain Configuration Mode.

```
Switch#configure terminal
Switch(config)#crypto pki certificate chain TP1
Switch(trustpoint)#
```

110-5 crypto pki certificate generate

This command is used to generate a new self-signed certificate.

crypto pki certificate generate

Parameters

None.

Default

By default, the Switch automatically generates a random build-in certificate.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to generate a new self-signed certificate regardless there is a build-in self-signed certificate or not. The Switch will generate a new self-signed certificate automatically if no certificate is detected after the Switch booted up.

The certificate generated by this command does not affect the user-downloaded certificates.



NOTE: This command only supports self-signature RSA certificate with the key length of 2048.

Example

This example shows how to generate a new self-signed certificate.

```
Switch#configure terminal
Switch(config)#crypto pki certificate generate

Start generating key ...
Start generating self-signed certificate ...
Done.
Switch(config)#
```

110-6 primary

This command is used to assign a specified trustpoint as the primary trustpoint of the Switch. Use the **no** form of this command to unbind the setting.

primary

no primary

Parameters

None.

Default

By default, this option is disabled.

Command Mode

CA-Trust-Point Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use the primary command to specify a given trustpoint as primary. This trustpoint can be used as default trustpoint when the application does not explicitly specify which certificate authority (CA) trustpoint should be used. Only one trustpoint can be specified as the primary. The last trustpoint specified as the primary will overwrite the previous one.

Example

This example shows how to configure the trustpoint “TP1” as the primary trustpoint.

```
Switch#configure terminal
Switch(config)#crypto pki trustpoint TP1
Switch(ca-trustpoint)#primary
Switch(ca-trustpoint)#
```

110-7 show crypto pki trustpoints

This command is used to display the trustpoints that are configured in the Switch.

show crypto pki trustpoints [*TRUSTPOINT***]**

Parameters

TRUSTPOINT	(Optional) Specifies the name of the trustpoint to be displayed.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If no parameter is specified, all trustpoints will be displayed.

Example

This example shows how to display all trustpoints.

```
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#
```

110-8 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

Privileged EXEC Mode.

Command Default Level

Level: 12.

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        : test
  Enabled Versions     :
    TLS 1.0
    TLS 1.1
    TLS 1.2
  Enabled CipherSuites :
    DHE_DSS_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_3DES_EDE_CBC_SHA,
    RSA_WITH_AES_128_CBC_SHA,
    RSA_WITH_AES_256_CBC_SHA,
    RSA_WITH_AES_128_CBC_SHA256,
    RSA_WITH_AES_256_CBC_SHA256,
    DHE_DSS_WITH_AES_256_CBC_SHA,
    DHE_RSA_WITH_AES_256_CBC_SHA
  Session Cache Timeout: 600
  Secure Trustpoint    :
Switch#
```

110-9 ssl-service-policy

This command is used to configure the SSL service policy. Use the **no** form of this command to remove the SSL service policy.

ssl-service-policy *POLICY-NAME* **[version [tls1.0] [tls1.1] [tls1.2]] | 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] [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha] | secure-trustpoint** *TRUSTPOINT* **| session-cache-timeout** *TIME-OUT***]**

no ssl-service-policy *POLICY-NAME* **[version [tls1.0] [tls1.1] [tls1.2]] | 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] [rsa-aes-128-cbc-sha] [rsa-aes-256-cbc-sha] [rsa-aes-128-cbc-sha256] [rsa-aes-256-cbc-sha256] [dhe-dss-aes-256-cbc-sha] [dhe-rsa-aes-256-cbc-sha] | secure-trustpoint | session-cache-timeout]**

Parameters

POLICY-NAME	Specifies the name of the SSL service policy.
version	(Optional) Specifies the TLS version. **tls1.0**- Indicate the appliance accepts TLS version 1.0. **tls1.1**- Indicate the appliance accepts TLS version 1.1. **tls1.2**- Indicate the appliance accepts TLS version 1.2.
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. **rsa-aes-128-cbc-sha** - Use RSA key exchange with AES 128-bit encryption for message encryption and SHA for message digest. **rsa-aes-256-cbc-sha** - Use RSA key exchange with AES 256-bit encryption for message encryption and SHA for message digest. **rsa-aes-128-cbc-sha256** - Use RSA key exchange with AES 128-bit encryption for message encryption and SHA 256 bits for message digest. **rsa-aes-256-cbc-sha256** - Use RSA key exchange with AES 256-bit encryption for message encryption and SHA 256 bits for message digest. **dhe-dss-aes-256-cbc-sha** - Use DH key exchange with AES 256-bit encryption for message encryption and SHA for message digest. **dhe-rsa-aes-256-cbc-sha** - Use DH key exchange with AES 256-bit encryption for message encryption and SHA 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 trustpoint that should be used in SSL handshake. When this parameter is not specified, the trustpoint which is specified as the primary will be used. If no primary trustpoint is specified, the built-in certificate/key pairs will be used. Use the **no** form of this command to cancel the specified trustpoint and use the built-in certificate/key pairs.
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 Use the **no** form of this command to revert the SSL session cache timeout to the default setting.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to configure the SSL service policy. When no optional parameter is specified and the specified policy name does not exist, a new SSL service policy is created and all optional parameters are associated with the policy with their default values.

Example

This example shows how to configure the SSL service policy “ssl-server” which associates the “TP1” trustpoint.

```
Switch#configure terminal
Switch(config)#ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

111. Unicast Reverse Path Forwarding (URPF) Commands

111-1 ip urpf

This command is used to enable 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** command is used to enable URPF globally and the **ip verify unicast source** command is used to enable URPF on the interface. To enable URPF on an interface, enable the function both globally and on the interface.

When enabled, the hardware routing table needs to be searched using the Session Initiation Protocol (SIP) first and then using the Dynamic Inspection Protocol (DIP). This is achieved by splitting the table into two halves so that the size of the IP routing table will be reduced by half. This will not take effect until the configuration was saved and the Switch was rebooted.

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)#
```

111-2 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 to the default settings

ip verify unicast source [reachable-via any] [access-group *IP-ACCESS-LIST-NAME***] [ipv6-access-group** *IPV6-ACCESS-LIST-NAME***]**

no ip verify unicast source [reachable-via] [access-group] [ipv6-access-group]

Parameters

reachable-via any	(Optional) Specifies how URPF verifies if the source address is present in the routing table of incoming packets (sometimes referred to as the loose mode).
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, no IPv4/IPv6 access list is specified.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for physical port interface configuration.

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 port 8.

```
Switch#configure terminal
Switch(config)#interface eth1/0/8
Switch(config-if)#ip verify unicast source
Switch(config-if)#
```

This example shows how to configure the Unicast RPF checking mode to any on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#ip verify unicast source reachable-via any
Switch(config-if)#
```

111-3 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 be displayed. Valid interfaces are physical interfaces.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 display the settings of URPF on ports 7 to 8.

```
Switch#show ip urpf 1/0/7-8

URPF Global State      : Enabled

Port      State     Reachable-  IP Access List Name
                    Via         IPv6 Access List Name
--------  --------  ----------  --------------------------------
1/0/7     Disabled  Any

1/0/8     Enabled   Any

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.
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.

112. Virtual LAN (VLAN) Commands

112-1 acceptable-frame

This command is used to set the acceptable types of frames by a port. Use the **no** form of this command to revert to the default 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** on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#acceptable-frame tagged-only
Switch(config-if)#
```

112-2 ingress-checking

This command is used to enable ingress checking for frames received by a port. Use the **no** form of this command to disable the ingress check.

ingress-checking

no ingress-checking

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

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 enable ingress checking on port 1.

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

112-3 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.
vlan *VLAN-ID*	Specifies the VLAN ID for the MAC-based VLAN entry.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If this parameter is not specified, the default CoS is 0.

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)#
```

112-4 protocol-vlan profile

This command is used to create a protocol group. Use the **no** form of this 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)#
```

112-5 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 this 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 *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 this parameter is 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 port 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)#
```

112-6 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 NETWORK-MASK*	Specifies the IPv4 network prefix and 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.
vlan *VLAN-ID*	Specifies the VLAN ID of the subnet VLAN.
priority *COS-VALUE*	(Optional) Specifies the priority CoS value. If this parameter is 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)#
```

112-7 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	Specifies the protocol group.
PROFILE-ID	(Optional) Specifies the protocol group to be displayed.
,	(Optional) Specifies a series of profile IDs or separates a range of profile IDs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of profile IDs. No space is allowed before or after the hyphen.
interface	Specifies the interfaces to be displayed.
INTERFACE-ID	(Optional) Specifies the port to display the protocol VLAN classification setting.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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 ports 1 to 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
 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)

Switch#
```

112-8 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.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the port to display the VLAN related setting.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
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/Privileged EXEC 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
   Description :
   Tagged Member Ports   :
   Untagged Member Ports : eth1/0/1-1/0/26

 Total Entries : 1

Switch#
```

This example shows how to display the PVID, ingress checking, and acceptable frame type information for ports 1 to 4.

```
Switch#show vlan interface eth1/0/1-4

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#
```

112-9 switchport access vlan

This command is used to specify the access VLAN for an interface. Use the **no** form of this command to revert to the default setting.

switchport access vlan *VLAN-ID*

no switchport access vlan

Parameters

VLAN-ID	Specifies the access VLAN of the interface.

Default

By default, this access VLAN is VLAN 1.

Command Mode

Interface Configuration Mode.

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 port 1 to access mode with access VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode access
Switch(config-if)#switchport access vlan 1000
Switch(config-if)#
```

112-10 switchport hybrid allowed vlan

This command is used to specify the tagged or untagged VLANs for a hybrid port. Use the **no** form of this command to revert to the default setting.

switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* **[, | -]**

no switchport hybrid allowed vlan

Parameters

add	(Optional) Specifies the port will be added into the specified VLAN(s).
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).
remove	Specifies the port will be removed from 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 parameter is specified, the specified VLAN list will overwrite the allowed VLAN list.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

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 port 1 to be a tagged member of VLAN 1000 and an untagged member of VLAN 2000 and 3000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add tagged 1000
Switch(config-if)#switchport hybrid allowed vlan add untagged 2000,3000
Switch(config-if)#
```

112-11 switchport hybrid native vlan

This command is used to specify the native VLAN ID of a hybrid port. Use the **no** form of this command to revert to the default setting.

switchport hybrid native vlan *VLAN-ID*

no switchport hybrid native vlan

Parameters

VLAN-ID	Specifies the native VLAN of a hybrid port.

Default

By default, the native VLAN of a hybrid port is VLAN 1.

Command Mode

Interface Configuration Mode.

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 port 1 to become a hybrid interface and configure the PVID to 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode hybrid
Switch(config-if)#switchport hybrid allowed vlan add untagged 1000,20
Switch(config-if)#switchport hybrid native vlan 20
Switch(config-if)#
```

112-12 switchport mode

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

switchport mode {access | hybrid | trunk | 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.



NOTE: When the switchport mode is **access**, only untagged packets can be forwarded through the MPLS Virtual Circuit (VC). To be able to forward both tagged and untagged packets through the MPLS VC, configure the switchport mode as **trunk**.

Example

This example shows how to configure port 1 as a trunk port.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#
```

112-13 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** form of this command to revert to the default setting.

switchport trunk allowed vlan {all | [add | remove | except] *VLAN-ID* **[, | -]}**

no switchport trunk allowed vlan

Parameters

all	Specifies that all VLANs are allowed on the interface.
add	(Optional) Specifies to add the specified VLAN list to the allowed VLAN list.
remove	(Optional) Specifies to remove the specified VLAN list from the allowed VLAN list.
except	(Optional) Specifies that all VLANs except the VLANs in the exception list are allowed.
VLAN-ID	Specifies the allow VLAN list or the VLAN list to be added to or removed from the allow VLAN list.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

By default, 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 port 1 as a tagged member of VLAN 1000.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk allowed vlan add 1000
Switch(config-if)#
```

112-14 switchport trunk native vlan

This command is used to specify the native VLAN ID of a trunk mode interface. Use the **no** form of this command to revert to the default setting.

switchport trunk native vlan {*VLAN-ID* **| tag}**

no switchport trunk native vlan [tag]

Parameters

VLAN-ID	Specifies the native VLAN for a trunk port.
tag	Specifies to enable the tagging mode of the native VLAN.

Default

By default, the native VLAN is 1, untagged mode.

Command Mode

Interface Configuration Mode.

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 port 1 as a trunk interface and configures the native VLAN to 20.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#switchport mode trunk
Switch(config-if)#switchport trunk native vlan 20
Switch(config-if)#
```

112-15 vlan

This command is used to add VLANs and enter the VLAN configuration mode. Use the **no** form of this command to remove VLANs.

vlan *VLAN-ID* **[, | -]**

no vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the ID of the VLAN to be added, removed or configured. The valid VLAN ID range is from 1 to 4094. VLAN ID 1 cannot be removed.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.

Default

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)#
```

112-16 vlan precedence

This command is used to specify the VLAN classification precedence for the port. Use the **no** form of this 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 port 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)#
```

112-17 name

This command is used to specify the name of a VLAN. Use the **no** form of this command to revert to the default setting.

name *VLAN-NAME*

no name

Parameters

VLAN-NAME	Specifies the VLAN name, with a maximum of 32 characters. The VLAN name must be unique within the administrative domain.

Default

The default VLAN name is VLANx, where x represents four numeric digits (including the leading zeros) that are equal to the VLAN ID.

Command Mode

VLAN Configuration Mode.

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)#
```

113. Virtual LAN (VLAN) Counter Commands

113-1 counting

This command is used to create a control entry for traffic statistics on specified Layer 2 VLAN interface(s). Use the **no** form of this command to delete the control entries.

counting [interface *INTERFACE-ID* **[, | -]] {broadcast | multicast |unicast | any} [rx | tx]**

no counting [interface *INTERFACE-ID* **[, | -]] [broadcast | multicast |unicast | any] [rx | tx]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the physical port interface(s) to be counted. If no physical port interface is specified, statistics is counted on merely a per-VLAN basis.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
broadcast	Specifies to count only broadcast frames.
multicast	Specifies to count only multicast frames.
unicast	Specifies to count only unicast frames.
any	Specifies to count all frames regardless of the frame type.
rx	(Optional) Specifies to count ingress traffic.
tx	(Optional) Specifies to count egress traffic.

Default

By default, no control entry is specified.

Command Mode

Layer 2 VLAN Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If no frame type is specified, the control entries is created or deleted based on the interfaces and traffic direction. If the traffic direction is not specified, both ingress and egress traffic will be counted.

This command is only valid for Layer 2 VLAN interface and it is used for products without proper hardware statistics resources per Layer 2 VLAN. This feature may share ACL resources.

Only physical port interfaces are valid for the optional interface parameter. The statistics is gathered on a per-VLAN basis if the interface is not specified. Alternatively it will count for specific physical port(s) in specific VLAN(s).

All of the control entries for specific VLAN(s) can be deleted using the **no counting** command without any parameters. All the control entries for specific physical port(s) in specific VLAN(s) can be deleted using the **no counting interface** *INTERFACE-ID* **[, | -]** command without succeeding parameters.

Example

This example shows how to create a control entry to count both ingress and egress statistics for VLAN 2.

```
Switch#configure terminal
Switch(config)#interface L2vlan 2
Switch(config-if)#counting any
Switch(config-if)#
```

This example shows how to create a control entry to count both ingress and egress broadcast statistics for VLAN 3.

```
Switch#configure terminal
Switch(config)#interface L2vlan 3
Switch(config-if)#counting broadcast
Switch(config-if)#
```

This example shows how to create a control entry to count ingress unicast statistics on port 1 in VLAN 5.

```
Switch#configure terminal
Switch(config)#interface L2vlan 5
Switch(config-if)#counting interface eth1/0/1 unicast rx
Switch(config-if)#
```

This example shows how to delete all control entries to count both ingress and egress statistics for VLAN 2.

```
Switch#configure terminal
Switch(config)#interface L2vlan 2
Switch(config-if)#no counting
Switch(config-if)#
```

This example shows how to delete all control entries to count both ingress and egress statistics on port 2 in VLAN 10.

```
Switch#configure terminal
Switch(config)#interface L2vlan 10
Switch(config-if)#no counting interface eth1/0/2
Switch(config-if)#
```

This example shows how to delete a control entry to count egress multicast statistics on port 10 in VLAN 20.

```
Switch#configure terminal
Switch(config)#interface L2vlan 20
Switch(config-if)#no counting interface eth1/0/10 multicast tx
Switch(config-if)#
```

113-2 show vlan counting

This command is used to display the control entries for the traffic statistics on specified Layer 2 VLAN interface(s).

show vlan counting [interface *INTERFACE-ID***] [rx | tx]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the Layer 2 VLAN interface(s) of the control entry to be displayed. If no Layer 2 VLAN interface is specified, all control entries will be displayed.

rx	(Optional) Specifies to display control entries for ingress traffic.
tx	(Optional) Specifies to display control entries for egress traffic.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the control entries for the traffic statistics on specified Layer 2 VLAN interface(s).

Example

This example shows how to display all Layer 2 VLAN statistics control entries.

```
Switch#show vlan counting

VLAN  Frame Type    Ports
----  ------------  -----------------------------------------------------
2     RX Unicast
3     RX Any
4     RX Multicast  1/0/1
10    RX Broadcast  1/0/1-1/0/5
2     TX Unicast
3     TX Any
4     TX Multicast  1/0/1
100   TX Broadcast  1/0/10-1/0/12

Total Entries: 8

Switch#
```

114. Virtual LAN (VLAN) Tunnel Commands

114-1 dot1q inner ethertype

This command is used to specify the system's inner TPID. Use the **no** form of this command to revert to the default setting.

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)#
```

114-2 dot1q tunneling ethertype

This command is used to specify the outer TPID for the service VLAN tag. Use the **no** form of this command to revert to the 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 port 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)#
```

114-3 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** form of this 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.
,	(Optional) Specifies a series of VLANs or separates a range of VLANs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before or after the hyphen.
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 this parameter is not specified, the priority of the service VLAN tag will be set to 0.

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)#
```

114-4 dot1q-tunnel insert dot1q-tag

This command is used to specify the dot1q VLAN tag insertion. Use the **no** form of this 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)#
```

114-5 vlan mapping miss drop

This command is used to enable the dropping of VLAN mapping unmatched packets. Use the **no** form of this 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)#
```

114-6 dot1q-tunnel trust inner-priority

This command is used to set the trusting dot1q priority. Use the **no** form of this 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)#
```

114-7 vlan mapping profile

This command is used to create a VLAN mapping profile or enter the VLAN mapping profile configuration mode. Use the **no** form of this 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 4.
type	(Optional) 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)#
```

114-8 vlan mapping rule

This command is used to configure the VLAN mapping rules of the profile. Use the **no** form of this 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 this parameter is not specified, the SN begins from 10 and the increment is 10. The SN range is from 1 to 10000
src-mac *MAC-ADDRESS*	(Optional) Specifies the source MAC address.
dst-mac *MAC-ADDRESS*	(Optional) Specifies the destination MAC address.
priority *COS-VALUE*	(Optional) Specifies the 802.1p priority.
inner-vid *VLAN-ID*	(Optional) Specifies the inner VLAN ID.
ether-type *VALUE*	(Optional) Specifies the Ethernet type.
src-ip *NETWORK-PREFIX*	(Optional) Specifies the source IPv4 address.
dst-ip *NETWORK-PREFIX*	(Optional) Specifies the destination IPv4 address.
src-ipv6 *IPV6-NETWORK-PREFIXIPREFIX-LENGTH*	(Optional) Specifies the source IPv6 address.
dst-ipv6 *IPV6-NETWORK-PREFIXIPREFIX-LENGTH*	(Optional) Specifies the destination IPv6 address.
dscp *VALUE*	(Optional) Specifies the DSCP value.
src-port *VALUE*	(Optional) Specifies the source TCP/UDP port number.
dst-port *VALUE*	(Optional) Specifies the destination TCP/UDP port number.
ip-protocol *VALUE*	(Optional) 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 this parameter is 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

Use this command 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)#
```

114-9 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 this 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)#
```

114-10 show dot1q ethertype

This command is used to display TPID settings.

show dot1q ethertype [*INTERFACE-ID* **[- | ,]]**

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC 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#
```

114-11 show dot1q-tunnel

This command is used to display the dot1q VLAN tunneling configuration on interfaces.

show dot1q-tunnel [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces that will be displayed. If this parameter is not specified, display all 802.1Q tunnel ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

114-12 show vlan mapping

This command is used to display the VLAN mapping configuration.

show vlan mapping [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interfaces that will be displayed. If this parameter is not specified, display the all VLAN mappings.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC 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#
```

114-13 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/Privileged EXEC 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#
```

115. Virtual Router Redundancy Protocol (VRRP) Commands

115-1 snmp-server enable traps vrrp

This command is used to enable the VRRP trap function in SNMP. Use the **no** form of this command to disable this function.

snmp-server enable traps vrrp [auth-fail] [new-master]

no snmp-server enable traps vrrp [new-master] [auth-fail]

Parameters

auth-fail	(Optional) Specifies the authentication failure trap status that will be configured. If the trap status is enabled, if a packet has been received from a router whose authentication key or authentication type conflicts with this router's authentication key or authentication type, a trap will be sent out.
new-master	(Optional) Specifies the new master trap status that will be configured. If the trap status is enabled, once the device has transitioned to the master state, a trap will be sent out.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to enable the VRRP trap state. If no parameter is specified, both trap types are enabled or disabled at the same time.

Example

This example shows how to enable the VRRP new master trap state.

```
Switch#configure terminal
Switch(config)#snmp-server enable traps vrrp new-master
Switch(config)#
```

115-2 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. This string can be up to 8 characters long.

Default

By default, no authentication is used.

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)#
```

115-3 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)#
```

115-4 vrrp priority

This command is used to configure the priority of the virtual router. Use the **no** form of this command to revert to the default setting.

vrrp *VRID* **priority** *PRIORITY*

no vrrp *VRID* **priority**

Parameters

VRID	Specifies the virtual router identifier. The range of value is from 1 to 255.
PRIORITY	Specifies the priority of the virtual router. The range of value is from 1 to 254.

Default

By default, the priority value is 100.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The master of a VRRP group is elected based on the priority. The virtual router with the highest priority becomes the master and others with lower priorities act as the backup for the VRRP group. If there are multiple routers with the same highest priority value, the router with the larger 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, and has the highest priority 255.

Example

This example shows how to configure the priority of the virtual router to 200.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#vrrp 1 priority 200
Switch(config-if)#
```

115-5 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 response.

vrrp non-owner-ping

no vrrp non-owner-ping

Parameters

None.

Default

By default, this option is disabled.

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)#
```

115-6 vrrp timers advertise

This command is used to configure the interval between successive VRRP advertisements by the master router. Use the **no** form of this command to revert to the default setting.

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 master 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)#
```

115-7 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 this 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, the preempt mode is used.

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 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)#
```

115-8 vrrp shutdown

This command is used to disable a virtual router on an interface. Use the **no** form of this command to revert to the default setting.

vrrp *VRID* **shutdown**

no vrrp *VRID* **shutdown**

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.

Default

By default, a virtual router is enabled after being created.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Avoid the common mistake of shutting down the IP address owner router before shutting down other non-owner routers.

Example

This example shows how to disable one VRRP VRID 1 on interface VLAN 1 while retaining the VRRP VRID 2.

```
Switch#configure terminal
Switch(config)#interface vlan 1
Switch(config-if)#vrrp 1 shutdown
Switch(config-if)#no vrrp 2 shutdown
Switch(config-if)#
```

115-9 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)#
```

115-10 show vrrp

This command is used to display the VRRP settings.

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/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the VRRP settings.

Example

This example shows how to display the VRRP settings.

```
Switch#show vrrp

vlan1 - Group 7 - Version2
  State is Master
  Virtual IP Address is 10.1.1.1
  Virtual MAC Address is 00-00-5E-00-01-07
  Advertisement interval is 10 seconds
  Preemption is enabled
  Priority is 100
  Authentication is enabled
  Authentication Text is test
  No critical IP address
  Master Router is 10.90.90.90(local)

Total Entries: 1
Switch#
```

115-11 show vrrp brief

This command is used to display the brief information of VRRP.

show vrrp brief

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the brief information of VRRP.

Example

This example shows how to display the brief information of VRRP.

```
Switch#show vrrp brief

Interface VRID Ver  AF  Pri Owner Pre State  VRouter IP
--------- ---- --- ---- --- ----- --- -----  ---------
vlan1      7    2  NA   100        Y  Master 10.1.1.1

Total Entries: 1
Switch#
```

115-12 debug vrrp

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

debug vrrp

no debug vrrp

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to enable or disable the VRRP debugging function.

Example

This example shows how to enable the VRRP debugging function.

```
Switch#debug vrrp
Switch#
```

115-13 debug vrrp errors

This command is used to enable the VRRP error debugging function. Use the **no** form of this command to disable this function.

debug vrrp errors

no debug vrrp errors

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to enable or disable the VRRP error debugging function.

Example

This example shows how to enable the VRRP error debugging function.

```
Switch#debug vrrp errors
Switch#
```

115-14 debug vrrp events

This command is used to enable the VRRP event debugging function. Use the **no** form of this command to disable this function.

debug vrrp events

no debug vrrp events

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to enable or disable the VRRP event debugging function. When enabled, debugging messages will be recorded when VRRP interface authentication or VRRP virtual MAC address is changed, or the Switch receives the specified VRRP advertisement.

Example

This example shows how to enable the VRRP event debugging function.

```
Switch#debug vrrp events
Switch#
```

115-15 debug vrrp packets

This command is used to enable the VRRP packet debugging function. Use the **no** form of this command to disable this function.

debug vrrp packets

no debug vrrp packets

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to enable or disable the VRRP packet debugging function. When enabled, debugging messages will be recorded when sending or receiving VRRP packets.

Example

This example shows how to enable the VRRP packet debugging function.

```
Switch#debug vrrp packets
Switch#
```

115-16 debug vrrp state

This command is used to enable the VRRP state debugging function. Use the **no** form of this command to disable this function.

debug vrrp state

no debug vrrp state

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to enable or disable the VRRP state debugging function. When enabled, debugging messages will be recorded when interface link, interface IP address, or VRRP state changes.

Example

This example shows how to enable the VRRP state debugging function.

```
Switch#debug vrrp state
Switch#
```

115-17 debug vrrp log

This command is used to enable the sending of VRRP log messages. Use the **no** form of this command to disable this function.

debug vrrp log

no debug vrrp log

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to enable or disable the sending of VRRP log messages.

Example

This example shows how to enable the sending of VRRP log messages.

```
Switch#debug vrrp log
Switch#
```

116. Virtual Router Redundancy Protocol Version 3 (VRRPv3) Commands

116-1 vrrp address-family

This command is used to create a VRRP virtual router and enter the IPv4 or IPv6 VRRP Address Family Configuration mode. Use the **no** form of this command to delete the group.

vrrp *VRID* **address-family {ipv4 | ipv6}**

no vrrp *VRID* **address-family {ipv4 | ipv6}**

Parameters

VRID	Specifies the virtual router identifier that identifies the VRRP group. The valid range is from 1 to 255.
ipv4	Specifies to create an IPv4 virtual router.
ipv6	Specifies to create an IPv6 virtual router.

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to create a VRRP virtual router and enter the IPv4 or IPv6 VRRP Address Family Configuration mode.

Example

This example shows how to create a VRRP virtual router and enter the IPv4 VRRP Address Family Configuration mode.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv4
Switch(config-af-vrrp)#
```

116-2 non-owner-ping

This command is used to enable a non-IP address owner virtual router in the master state to response the ICMP echo request for IPv4 address or the ND request for IPv6 address. Use the **no** form of this command to disable the function.

non-owner-ping

no non-owner-ping

Parameters

None.

Default

By default, this option is disabled.

Command Mode

VRRP Address Family Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable or disable a non-IP address owner virtual router in the master state to response the ICMP echo request for IPv4 address or the ND request for IPv6 address.

Example

This example shows how to enable the non-owner ping function.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#non-owner-ping
Switch(config-af-vrrp)#
```

116-3 address

This command is used to configure the virtual IPv4 or IPv6 address for one virtual router. Use the **no** form of this command to delete the virtual address.

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

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

Parameters

IP-ADDRESS	Specifies the virtual IPv4 address of the virtual router.
IPv6-ADDRESS	Specifies the virtual IPv6 address of the virtual router.

Default

None.

Command Mode

VRRP Address Family Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the virtual IPv4 or IPv6 address for one virtual router. All routers in the same VRRP group must be configured with the same virtual router ID and virtual address. The IP address of the virtual router can be a real address configured on the routers or an unused address. If the virtual address is equal to the real address of the interface, this virtual router is the IP address owner.

Example

This example shows how to configure a virtual IPv6 address on a VRRP group.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#address FE80::2
Switch(config-af-vrrp)#
```

116-4 priority

This command is used to configure the priority of the virtual router. Use the **no** form of this command to revert to the default setting.

priority *PRIORITY*

no priority

Parameters

PRIORITY	Specifies the priority of the virtual router. The range of value is from 1 to 254.

Default

By default, the value is 100.

Command Mode

VRRP Address Family Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The master of a VRRP group is elected based on the priority. The virtual router with the highest priority becomes the master and others with lower priorities act as the backup for the VRRP group. If there are multiple routers with the same highest priority value, the router with the larger 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, and has the highest priority 255.

Example

This example shows how to configure the priority to 200.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#priority 200
Switch(config-af-vrrp)#
```

116-5 timers advertise

This command is used to configure the interval between successive VRRP advertisements. Use the **no** form of this command to revert to the default setting.

timers advertise *INTERVAL*

no timers advertise

Parameters

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

VRRP Address Family Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The maser will constantly send VRRP advertisements. All virtual 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 1 every 10 seconds on interface VLAN 3.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#timers advertise 10
Switch(config-af-vrrp)#
```

116-6 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 this command to change back to non-preempt mode.

preempt

no preempt

Parameters

None.

Default

By default, the preempt mode is used.

Command Mode

VRRP Address Family Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **no preempt** command to disable preemption in order to keep the VRRP group stable.

Example

This example shows how to disable preemption.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#no preempt
Switch(config-af-vrrp)#
```

116-7 shutdown

This command is used to disable a virtual router. Use the **no** form of this command to revert to the default setting.

shutdown

no shutdown

Parameters

None.

Default

By default, a virtual router is enabled after being created.

Command Mode

VRRP Address Family Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Avoid the common mistake of shutting down the IP address owner router before shutting down other non-owner routers.

Example

This example shows how to disable one virtual router on interface VLAN 3.

```
Switch#configure terminal
Switch(config)#interface vlan3
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#shutdown
Switch(config-af-vrrp)#
```

116-8 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.

track critical-ip {*IP-ADDRESS* **| [***INTERFACE-ID***]** *IPV6-ADDRESS***}**

no track critical-ip

Parameters

IP-ADDRESS	Specifies the critical IP address.
INTERFACE-ID	(Optional) Specifies the interface of critical IP address to be used.
IPv6-ADDRESS	Specifies the critical IPv6 address.

Default

None.

Command Mode

VRRP Address Family 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 IPv6 address of virtual router 1 on VLAN 1.

```
Switch#configure terminal
Switch(config)#interface vlan1
Switch(config-if)#vrrp 1 address-family ipv6
Switch(config-af-vrrp)#track critical-ip vlan1 FE80::2
Switch(config-af-vrrp)#
```

116-9 show vrrp

This command is used to display the VRRP settings and status.

show vrrp [interface *INTERFACE-ID* **[***VRID***]] [ipv4 | ipv6]**

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.
ipv4	(Optional) Specifies to only display the information of the IPv4 virtual routers.
ipv6	(Optional) Specifies to only display the information of the IPv6 virtual routers.

Default

None.

Command Mode

User/Privileged EXEC 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

vlan3 - Group 1 - Version3 - Address-Family IPv6
  State is Init
  Virtual IP Address is ::
  Virtual MAC Address is 00-00-5E-00-02-01
  Advertisement interval is 1 seconds
  Preemption is enabled
  Priority is 100
  No critical IP address
  Disable non owner ping
  Master Router is ::


Total Entries: 1


Switch#
```

116-10 show vrrp brief

This command is used to display the VRRP brief information.

show vrrp brief

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC 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 Ver  AF   Pri Owner Pre State  VRouter IP
--------- ---- --- ---- --- ----- --- -----  ---------
vlan3      1    3  IPv6 100        Y  Init   ::

Total Entries: 1


Switch#
```

117. Voice VLAN Commands

117-1 voice vlan

This command is used to enable the global voice VLAN state and configure the voice VLAN. Use the **no** form of this command to disable the voice VLAN state.

voice vlan *VLAN-ID*

no voice vlan

Parameters

VLAN-ID	Specifies the ID of the voice VLAN. The valid range is from 2 to 4094.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to enable the global voice VLAN function and to specify the voice VLAN on the Switch. The Switch has only one voice VLAN.

Both the **voice vlan** command in the global configuration and the **voice vlan enable** command in the interface configuration mode need to be enabled for a port to start the voice VLAN function.

When the voice VLAN is enabled for a port, the received voice packets will be forwarded in the voice VLAN. The received packets are determined as voice packets if the source MAC addresses of packets comply with the organizationally unique identifier (OUI) addresses configured by the **voice vlan mac-address** command.

The VLAN to be specified as the voice VLAN needs to pre-exist before configuration. If the voice VLAN is configured, the voice VLAN cannot be removed with the **no vlan** command.

Example

This example shows how to enable the voice VLAN function and configure VLAN 1000 as the voice VLAN.

```
Switch#configure terminal
Switch(config)#voice vlan 1000
Switch(config)#
```

117-2 voice vlan aging

This command is used to configure the aging time for aging out the voice VLAN's dynamic member ports. Use the **no** form of this command to revert to the default setting.

voice vlan aging *MINUTES*

no voice vlan aging

Parameters

MINUTES	Specifies the aging time of the voice VLAN. The valid range is from 1 to 65535 minutes.

Default

By default, this value is 720 minutes.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the aging time for aging out the voice device and the voice VLAN automatically learned member ports. When the last voice device connected to the port stops sending traffic and the MAC address of this voice device is aged out from FDB, the voice VLAN aging timer will be started. The port will be removed from the voice VLAN after the expiration of the voice VLAN aging timer. If voice traffic resumes during the aging time, the aging timer will be cancelled.

Example

This example shows how to configure the aging time of the voice VLAN to 30 minutes.

```
Switch#configure terminal
Switch(config)#voice vlan aging 30
Switch(config)#
```

117-3 voice vlan enable

This command is used to enable the voice VLAN state of ports. Use the **no** form of this command to disable the voice VLAN's port state.

voice vlan enable

no voice vlan enable

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command takes effect for access ports or hybrid ports. Use the **voice vlan enable** command to enable the voice VLAN function for ports. Both the **voice vlan** command in the global configuration and the **voice vlan enable** command in the interface configuration mode need to be enabled for a port to start the voice VLAN function.

Example

This example shows how to enable the voice VLAN function on port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan enable
Switch(config-if)#
```

117-4 voice vlan mac-address

This command is used to add the user-defined voice device OUI. Use the **no** form of this command to delete the user-defined voice device OUI.

voice vlan mac-address *MAC-ADDRESS MASK* **[description** *TEXT***]**

no voice vlan mac-address *MAC-ADDRESS MASK*

Parameters

MAC-ADDRES	Specifies the OUI MAC address.
MASK	Specifies the OUI MAC address matching bitmask.
description *TEXT*	(Optional) Specifies the description for the user defined OUI with a maximum of 32 characters.

Default

The default OUI is listed in the following table:

OUI	Vendor
00:E0:BB	3COM
00:03:6B	Cisco
00:E0:75	Veritel
00:D0:1E	Pingtel
00:01:E3	Siemens
00:60:B9	NEC/Philips
00:0F:E2	Huawei-3COM
00:09:6E	Avaya

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to add a user-defined OUI for the voice VLAN. The OUI for the voice VLAN is used to identify the voice traffic by using the voice VLAN function. If the source MAC addresses of the received packet matches any of the OUI patterns, the received packet is determined as a voice packet.

The user-defined OUI cannot be the same as the default OUI. The default OUI cannot be deleted.

Example

This example shows how to add a user-defined OUI for voice devices.

```
Switch#configure terminal
Switch(config)#voice vlan mac-address 00-02-03-00-00-00 FF-FF-FF-00-00-00 description User1
Switch(config)#
```

117-5 voice vlan mode

This command is used to enable the automatic learning of the port as voice VLAN member ports. Use the **no** form of this command to disable the automatic learning.

voice vlan mode {manual | auto {tag | untag}}

no voice vlan mode

Parameters

manual	Specifies that voice VLAN membership will be manually configured.
auto	Specifies that voice VLAN membership will be automatically learned.
tag	Specifies to learn voice VLAN tagged members.
untag	Specifies to learn voice VLAN untagged members.

Default

By default, this option is set to **untag** and **auto**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure automatic learning or manual configuration of voice VLAN member ports.

If auto-learning is enabled, the port will automatically be learned as a voice VLAN member. This membership will be automatically be aged out. When the port is working in the **auto tagged** mode and the port captures a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in port's PVID VLAN.

When the port is working in **auto untagged** mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them in voice VLAN.

When the Switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag, and priority flag. The Switch should follow the tagged flag and priority setting.

If auto learning is disabled, the user should use the **switchport hybrid vlan** command to configure the port as a voice VLAN tagged or untagged member port.

Example

This example shows how to configure port 1 to be in the **auto tag** mode.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#voice vlan mode auto tag
Switch(config-if)#
```

117-6 voice vlan qos

This command is used to configure the CoS priority for the incoming voice VLAN traffic. Use the **no** form of this command to revert to the default setting.

voice vlan qos *COS-VALUE*

no voice vlan qos

Parameters

COS-VALUE	Specifies the priority of the voice VLAN. This value must be between 0 and 7.

Default

By default, this value is 5.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The voice packets arriving at the voice VLAN enabled port are marked to the CoS specified by the command. The remarking of CoS allows the voice VLAN traffic to be distinguished from data traffic in quality of service.

Example

This example shows how to configure the priority of the voice VLAN to be 7.

```
Switch#configure terminal
Switch(config)#voice vlan qos 7
Switch(config)#
```

117-7 show voice vlan

This command is used to display the voice VLAN configurations.

show voice vlan [interface [*INTERFACE-ID* **[, | -]]]**

show voice vlan {device | lldp-med device} [interface *INTERFACE-ID* **[, | -]]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies to display voice VLAN information of ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
device	Specifies to display the voice devices learned by OUI.
lldp-med device	Specifies to display the voice devices learned by LLDP-MED.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the voice VLAN configurations.

Example

This example shows how to display the voice VLAN global settings.

```
Switch#show voice vlan

 Voice VLAN ID        : 3
 Voice VLAN CoS       : 5
 Aging Time           : 720 minutes
 Member Ports         : 1/0/1-1/0/5
 Dynamic Member Ports : 1/0/1-1/0/3

 Voice VLAN OUI       :

OUI Address        Mask               Description
 -----------------  -----------------  --------------
 00-01-E3-00-00-00  FF-FF-FF-00-00-00  Siemens
 00-02-03-00-00-00  FF-FF-FF-00-00-00  User1
 00-03-6B-00-00-00  FF-FF-FF-00-00-00  Cisco
 00-09-6E-00-00-00  FF-FF-FF-00-00-00  Avaya
 00-0F-E2-00-00-00  FF-FF-FF-00-00-00  Huawei&3COM
 00-60-B9-00-00-00  FF-FF-FF-00-00-00  NEC&Philips
 00-D0-1E-00-00-00  FF-FF-FF-00-00-00  Pingtel
 00-E0-75-00-00-00  FF-FF-FF-00-00-00  Veritel
 00-E0-BB-00-00-00  FF-FF-FF-00-00-00  3COM

 Total OUI: 9

Switch#
```

This example shows how to display the voice VLAN information of ports.

```
Switch#show voice vlan interface eth1/0/6-10

 Interface       State     Mode
 --------------  --------  -----------
 eth1/0/6        Enabled   Manual
 eth1/0/7        Enabled   Manual
 eth1/0/8        Enabled   Manual
 eth1/0/9        Enabled   Manual
 eth1/0/10       Disabled  Auto/Untag

Switch#
```

This example shows how to display the learned voice devices on ports 1 to 2.

```
Switch#show voice vlan device interface eth1/0/1-2

 Interface       Voice Device       Start Time        Status
 --------------  -----------------  ----------------  ------
 eth1/0/1        00-03-6B-00-00-01  2012-03-19 09:00   Active
 eth1/0/1        00-03-6B-00-00-02  2012-03-20 10:09   Aging
 eth1/0/1        00-03-6B-00-00-05  2012-03-20 12:04   Active
 eth1/0/2        00-03-6B-00-00-0a  2012-03-19 08:11   Aging
 eth1/0/2        33-00-61-10-00-11  2012-03-20 06:45   Aging

Total Entries: 5

Switch#
```

This example shows how to display the learned LLDP-MED voice devices on ports 1 to 2.

```
Switch#show voice vlan lldp-med device interface eth1/0/1-2

Index                 : 1
Interface             : eth1/0/1
Chassis ID Subtype    : MAC Address
Chassis ID            : 00-E0-BB-00-00-11
Port ID Subtype       : Network Address
Port ID               : 172.18.1.1
Create Time           : 2012-03-19 10:00:00
Remain Time           : 108 Seconds

Index                 : 2
Interface             : eth1/0/2
Chassis ID Subtype    : MAC Address
Chassis ID            : 00-E0-BB-00-00-12
Port ID Subtype       : Network Address
Port ID               : 172.18.1.2
Create Time           : 2012-03-20 11:00:00
Remain Time           : 105 Seconds

Total Entries: 2
Switch#
```

118. Web Authentication Commands

118-1 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 port 1.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#web-auth enable
Switch(config-if)#
```

118-2 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 successfully log into 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 @ 2022 All Rights Reserved

Line 2: Site: http://support.website.com

```
Switch#configure terminal
Switch(config)#web-auth page-element copyright-line 1 title Copyright @ 2022 All Rights Reserved
Switch(config)#web-auth page-element copyright-line 2 title Site: http://support.website.com
Switch(config)#
```

118-3 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)#
```

118-4 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)#
```

118-5 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 revert 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 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)#
```

118-6 snmp-server enable traps web-auth

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

snmp-server enable traps web-auth

no snmp-server enable traps web-auth

Parameters

None.

Default

By default, this feature is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

None.

Example

This example shows how to enable the sending of SNMP notifications for Web authentication

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

---

119. Weighted Random Early Detection (WRED) Commands

119-1 random-detect

This command is used to enable the WRED function. Use the **no** form of this command 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 this parameter is 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.

$$Drop\ \Pr obability = \frac{avg\_Qsize - MinThreshold}{MaxThreshold - MinThreshold} * MaxDropRate$$

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, the default setting of the threshold will be associated.

Example

This example shows how to enable the WRED function on Port 1 queue 5 and apply the WRED profile 10.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#random-detect 5 profile 10
Switch(config-if)#
```

119-2 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 this command to revert 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 port 1 queue 5.

```
Switch#configure terminal
Switch(config)#interface eth1/0/1
Switch(config-if)#random-detect exponential-weight 5 exponent 10
Switch(config-if)#
```

119-3 random-detect profile

This command is used to configure the WRED profile. Use the **no** form of this command to revert to the default setting.

random-detect profile *ID* **[tcp] [green | yellow | red] min-threshold** *VALUE* **max-threshold** *VALUE* **max-drop-rate** *VALUE*

no random-detect profile *ID*

Parameters

ID	Specifies the ID of the WRED profile that will be set.
tcp	(Optional) Specifies the WRED drop parameters for the TCP packets to be set.
green	(Optional) Specifies the WRED drop parameters for green packets to be set.

yellow	(Optional) Specifies the WRED drop parameters for yellow packets to be set.
red	(Optional) 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, the packet will not be dropped or remarked for ECN. The range is from 0 to 14, where 0 to 10 represents 0% to 10%, 11 represents 25%, 12 represents 50%, 13 represents 75%, and 14 represents 100%.

Default

The minimum threshold is 20.

The maximum threshold is 80.

The maximum drop rate is 0.

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 packets on profile 10.

```
Switch#configure terminal
Switch(config)#random-detect profile 10 tcp yellow min-threshold 20 max-threshold 40 max-drop-rate 5
Switch(config)#
```

119-4 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.

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

Default

None.

Command Mode

User/Privileged EXEC 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 port 1.

```
Switch#show queueing random-detect interface eth1/0/1

 Current WRED configuration:

   eth1/0/1
   CoS  WRED State  Exp-weight-constant  Profile
   ---  ----------  -------------------  -------
   0    Disabled    9                    1
   1    Disabled    9                    1
   2    Disabled    9                    1
   3    Disabled    9                    1
   4    Disabled    9                    1
   5    Disabled    9                    1
   6    Disabled    9                    1
   7    Disabled    9                    1

Switch#
```

119-5 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 this parameter is not specified, the configuration for all WRED profiles will be displayed.

Default

None.

Command Mode

User/Privileged EXEC 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        20             80             1
 TCP-YELLOW       20             80             5
 TCP-RED          20             80             8
 NON-TCP-GREEN    20             80             10
 NON-TCP-YELLOW   20             80             10
 NON-TCP-RED      20             80             10

Switch#
```

120. Zone Defense Commands

120-1 zone-defense

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

zone-defense

no zone-defense

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 or disable the zone defense function. When enabled, the ACL resource will be reserved for the zone defense. The zone defense function cannot be enabled if the Switch does not have enough ACL resource.

Example

This example shows how to enable the zone defense function.

```
Switch#configure terminal
Switch(config)#zone-defense
Switch(config)#
```

120-2 show zone_defense

This command is used to display the zone defense state.

show zone_defense

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to display the zone defense state.

Example

This example shows how to display the zone defense state.

```
Switch#show zone_defense

Zone Defense Status           : Enabled


Switch#
```

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DGS-1520 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                                          1.00.011
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address    : 80-26-89-15-28-00
  H/W Version    : A1

  Please Wait, Loading V1.01.004 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. The possible reason may be: (1) user authentication failure. (2) no server(s) responding. (3) no servers configured. (4) no resources. (5) user timeout expired. username: The user that is being authenticated. interface-id: The interface name. macaddr: The MAC address of the authenticated device.	Critical
Event Description: 802.1X Authentication successful. Log Message: 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: 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: Successful login. 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: Login failed.	Warning

Log Message: Login 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.: 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.	
Event Description: Login failed due to AAA server timeout or improper configuration. 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 if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event Description: 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: 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.: 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.	Warning
Event Description: 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 if authentication method is remote server. username: It indicates the username for authentication.	Warning
Event Description: 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.	Informational

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.	
Event Description: 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: RADIUS assigned a valid priority attributes. Log Message: RADIUS server <server-ip> assigned 802.1p default priority: <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: 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
Event Description: This log will be generated when RADIUS assigned ACL script is applied to the system due to insufficient resource. Log Message" RADIUS server <server-ip> assigns <username> ACL success 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.	Informational

ARP

Log Description	Severity
Event Description: Gratuitous ARP detected duplicate IP. Log Message: Conflict IP was detected with this device (IP: <ipaddr>, MAC: <macaddr>, Port <[unitID:]portNum>, Interface: <ipif_name>) Parameters Description: ipaddr: The IP address which is duplicated with our device. macaddr: The MAC address of the device that has duplicated IP address as our device. unitID: 1.Interger value;2.Represent the id of the device in the stacking system. portNum: 1.Interger value;2.Represent the logic port number of the device.	Warning

ipif_name: The name of the interface of the switch which has the conflict IP address.

ARP Spoofing Prevention

Log Description	Severity
Event Description: a fake ARP packet detect by ARP Spoofing Prevention. Log Message: Gateway <ipaddr> is under attack by <macaddr> from <interface-id> Parameters Description: ipaddr: The IP address of gateway. macaddr: The MAC address of hacker. interface-id: The interface where hacker is located.	Warning

Auto Image

Log Description	Severity
Event Description: This message means that Autoimage Firmware upgraded successfully. Log Message: The downloaded firmware was successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: TFTP Server IP address.	Informational
Event Description: This message means that Autoimage Firmware upgraded unsuccessfully. Log Message: The downloaded firmware was not successfully executed by DHCP AutoImage update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: TFTP Server IP address.	Informational

Auto Save

Log Description	Severity
Event Description: Record the event when the configure information of DDP is saved automatically. Log Message:CONFIG-6-DDPSAVECONFIG: [Unit <unitID>,]Configuration automatically saved to flash due to configuring from DDP(Username: <username>, IP: <ipaddr>) Parameters Description: Unit: Box ID. username: Represent current login user. ipaddr: Represent client IP address.	Informational

Auto Surveillance VLAN

Log Description	Severity
Event Description: When a new surveillance device is detected on an interface. Log Message: New surveillance device detected (<interface-id>, MAC: <mac-address>)	Informational

Parameters Description: interface-id: Interface name. mac-address: Surveillance device MAC address.	
Event Description: When an interface which is enabled surveillance VLAN joins the surveillance VLAN automatically. Log Message: <interface-id> add into surveillance VLAN <vid> Parameters Description: interface-id: Interface name. vid: VLAN ID.	Informational
Event Description: When an interface leaves the surveillance VLAN and at the same time, no surveillance device is detected in the aging interval for that interface, the log message will be sent. Log Message: <interface-id> remove from surveillance VLAN <vid> Parameters Description: interface-id: Interface name. vid: VLAN ID.	Informational

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

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>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event Description: Firmware upgraded unsuccessfully. Log Message: [Unit <unitID>,]Firmware upgraded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>)	Warning

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. serverIP: Server IP address. pathFile: Path and file name on server.	
Event Description: Firmware uploaded successfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> successfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event Description: Firmware uploaded unsuccessfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event Description: Configuration downloaded successfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event Description: Configuration downloaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	
Event Description: Configuration uploaded successfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event Description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event Description: Configuration saved to flash by console. Log Message: [Unit <unitID>,]Configuration saved to flash by console (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Log message uploaded successfully. Log Message: [Unit <unitID>,] Log message uploaded by <session> successfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: unitID: The unit ID. session: The user's session. username: The current login user. ipaddr: The client IP address. macaddr: The client MAC address.	Informational
Event Description: Log message uploaded unsuccessfully. Log Message: [Unit <unitID>,] Log message uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>]) Parameters Description: unitID: The unit ID. session: The user's session. username: The current login user. ipaddr: The client IP address. macaddr: The client MAC address.	Warning

Event Description: Configuration saved to flash by remote. Log Message: [Unit <unitID>,]Configuration saved to flash (Username: <username>, IP: <ipaddr>) Parameters Description: unitID: The unit ID. username: The current login user. ipaddr: The client IP address.	Informational
Event Description: Unknown type files downloaded unsuccessfully. Log Message: [Unit <unitID>,]Downloaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) 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. serverIP: Server IP address. pathFile: Path and file name on server.	Warning

NOTE: 1. The user's session refers to Console, Web, SNMP, Telnet, SSH, and DDP sessions.
2. If the Switch is in the standalone state, there will be no unit ID in the log message.
3. If the configuration or firmware was downloaded or uploaded through the console, there will be no IP address and MAC address information in the log message.

DAD

Log Description	Severity
Event Description: When DUT receives Neighbor Solicitation (NS) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Solicitation Messages Parameters Description: ipv6address: IPv6 address in Neighbor Solicitation Messages. interface-id: port interface ID.	Warning
Event Description: When DUT receives Neighbor Advertisement (NA) message with reduplicated address in the DAD duration, DUT will add a log. Log Message: Duplicate address <ipv6address> on <interface-id> via receiving Neighbor Advertisement Messages Parameters Description: ipv6address: IPv6 address in Neighbor Advertisement Messages. interface-id: port interface ID.	Warning

DAI

Log Description	Severity

Event Description: Detect illegal 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. ipaddr: IP address. macaddr: MAC address. vlanid: VLAN ID. interface-id: Interface name.	Warning
Event Description: Detect legal 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. ipaddr: IP address. macaddr: MAC address. vlanid: VLAN ID. interface-id: Interface name.	Informational

DDM

Log Description	Severity
Event Description: when the any of SFP parameters exceeds from the warning threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> warning threshold exceeded Parameters Description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Warning
Event Description: when the any of SFP parameters exceeds from the alarm threshold. Log Message: Optical transceiver <interface-id> <component> <high-low> alarm threshold exceeded Parameters Description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power high-low: High or low threshold.	Critical

Event Description: when the any of SFP parameters recovers from the warning threshold. Log Message: Optical transceiver <interface-id> <component> back to normal Parameters Description: interface-id: port interface ID. component: DDM threshold type. It can be one of the following types: temperature supply voltage bias current TX power RX power	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: 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 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.	Informational

ipif-name: Name of the DHCPv6 client interface.	
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 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 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 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 interface.	Informational
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

DNS Resolver

Log Description	Severity
Event Description: Duplicate Domain name cache added, leads a dynamic domain name cache be deleted. Log Message: Duplicate Domain name case name: <domainname>, static IP: <ipaddr>, dynamic IP:<ipaddr> Parameters Description: domainname: the domain name string. ipaddr: IP address.	Informational

DoS Prevention

Log Description	Severity
Event Description: Detect DOS attack. Log Message: <dos-type> is dropped from (IP: <ip-address> Port <interface-id>) Parameters Description: dos-type: DOS attack type. ip-address: IP address. interface-id: Interface name.	Notification

Errdisable

Log Description	Severity
Event Description: When a port enter error disable state. Log Message: Port <interface-id> enters error disable state due to <reason-id> Parameters Description: interface-id: The port number.	Warning

reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Digital Diagnostics Monitoring, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	
Event Description: When a port leaves error disable state. Log Message: Port <interface-id> leaves the error disable state which is previously caused by <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving.	Warning
Event Description: When a port enter error disable state. Log Message: Port <interface-id> VLAN <vid> enters error disable state due to <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid: VLAN ID.	Warning
Event Description: When a port leaves error disable state. Log Message: Port <interface-id> VLAN <vid> leaves the error disable state which is previously caused by <reason-id> Parameters Description: interface-id: The port number. reason-id: Loopback Detection, Port Security Violation, Storm Control, BPDU Protect, ARP Rate Limit, DHCP Rate Limit, L2 Protocol Tunneling, Scheduled Port-shutdown by Power Saving, Scheduled Hibernation by Power Saving. vid: VLAN ID.	Warning

Interface

Log Description	Severity
Event Description: When port is down. Log Message: Port <port-type>< interface-id> link down Parameters Description: port-type: Port type. interface-id: Interface name.	Informational
Event Description: When port is up. Log Message: Port <port-type>< interface-id> link up, <link-speed> Parameters Description: port-type: Port type. interface-id: Interface name. link-speed: Port link speed.	Informational

IP Source Guard

Log Description	Severity

Event Description: When there is no hardware rule resource to set DHCP Snooping entry into IPSG table, the syslog will be record. Log Message: Failed to set IPSG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>) Parameters Description: ipaddr: IP address. macaddr: MAC address. vlanid: VLAN ID. interface-id: Interface name.	Warning

IPv6 Snooping

Log Description	Severity
Event Description: IPv6 data glean failed. Log Message: Failed to glean (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) Parameters Description: IPADDR: The IP address of IPv6 Snooping entry. MACADDR: The MAC address of IPv6 Snooping entry. VLANID: The VID of IPv6 Snooping entry. INTERFACE_ID: The port of IPv6 Snooping entry.	Notification
Event Description: IPv6 data glean succeeded. Log Message: Glean to recover (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Port <INTERFACE-ID>) Parameters Description: IPADDR: The IP address of IPv6 Snooping entry. MACADDR: The MAC address of IPv6 Snooping entry. VLANID: The VID of IPv6 Snooping entry. INTERFACE_ID: The port of IPv6 Snooping entry.	Informational

IPv6 Source Guard

Log Description	Severity
Event Description: When there is no hardware rule resource to set IPv6 Snooping entry into IPv6SG table, the syslog will be record. Log Message: Failed to set IPv6SG entry due to no hardware rule resource. (IP: <IPADDR>, MAC: <MACADDR>, VID: <VLANID>, Interface <INTERFACE-ID>) Parameters Description: ipaddr: The IPv6 address of IPv6 Snooping entry. macaddr: The MAC address of IPv6 Snooping entry. vlanid: The VID of IPv6 Snooping entry. interface-id: The interface of IPv6 Snooping entry.	**Warning**

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up.	Informational

Log Message: Link Aggregation Group <group_id> link up Parameters Description: group_id: The group id of the link up aggregation group.	
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 Parameters Description: interface-id: Interface on which loop is detected.	Critical
Event Description: Record the event when an interface detect loop. Log Message: <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 Parameters Description: interface-id: Interface on which loop is detected.	Critical
Event Description: Record the event when an interface loop recovered. Log Message: interface-id> VLAN <vlan-id> LBD loop recovered 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 the number of VLANs that loop back has occurred exceeds a reserved number. Log Message: Loop VLAN numbers overflow	Critical

LLDP-MED

Log Description	Severity
Event Description: LLDP-MED topology change detected.	Notification

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.

Event Description: Conflict LLDP-MED device type detected.	Notification

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.

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.	Notification

Login/Logout

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>)	Informational

Parameters Description: unitID: The unit ID. username: Represent current login user.	
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-based Access Control

Log Description	Severity
Event Description: A host has passed MAC authentication.	Informational

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.	
Event Description: A 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: A host failed to pass the authentication. Log Message: MAC-based Access Control host login fail (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.	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

MSTP Debug

Log Description	Severity
Event Description: Used to record the event that Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
Event Description: Used to record the event that Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
Event Description: Used to record MSTP instance topology change event. Log Message: Topology changed (Instance : <Instance-id>,<interface_id>, MAC:<macaddr>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	Notification

interface_id: The port number which detect or receive topochange information. macaddr: The system of bridge mac address.	
Event Description: Used to record MSTP instance new root bridge selected. Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <Instance-id>] MAC: <macaddr> Priority :<priority>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. macaddr: The system of bridge mac address. priority: The bridge priority value must be divisible by 4096.	Informational
Event Description: Used to record MSTP instance new root port selected. Log Message: New root port selected (Instance:<Instance-id>, <interface_id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. interface_id: The port number which detect or receive topochange information.	Notification
Event Description: Used to record MSTP instance port state change event. Log Message: Spanning Tree port status change (Instance :<Instance-id>, <interface_id>) <old_status> -> <new_status> Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. interface_id: The port number which detect or receive topochange information. old status: new status: The port of STP state. The value may be Disable, Discarding, Learning, Forwarding.	Notice
Event Description: Used to record MSTP instance port role change event. Log Message: Spanning Tree port role change (Instance :<Instance-id>, <interface_id>) <old_role> -> <new_role> Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. Interface_id: The port number which detect or receive topochange information. old role: new role : The port role of stp. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	Informational
Event Description: Use to record action to create an MST instance. Log Message: Spanning Tree instance created (Instance :<Instance-id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	Informational
Event Description: Use to record action to delete an MST instance. Log Message: Spanning Tree instance deleted (Instance :<Instance-id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST.	Informational
Event Description: Use to record action to change the STP version. Log Message: Spanning Tree version change (new version :<new_version>) Parameters Description: new_version: Running under which version of STP.	Informational
Event Description: Used to record the configuration name and revision level changed in the MST Configuration Identification. Log Message: Spanning Tree MST configuration ID name and revision level change (name: <name>, revision level <revision_level>) Parameters Description: name: The name given for a specified MST region.	Informational

revision_level: Switches using the same given name but with a different revision level are considered members of different MST regions.	
Event Description: Use to record action to maps a VLAN(s) to an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. startvlanid: The start vid of add vlan range. endvlanid: The end vid of add vlan range.	Informational
Event Description: Use to record action to delete a VLAN(s) from an MST instance. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <Instance-id> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. startvlanid: The start vid of delete vlan range. endvlanid: The end vid of delete vlan range.	Informational
Event Description: Used to record the event that port role change to alternate due to guard root. Log Message: Spanning Tree port role change (Instance :<instance-id>, <interface-id>) to alternate port due to the guard root Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. Interface_id: The port number which detect the event.	Informational
Event Description: Used to record the event that port change to blocking state due to loop guard. Log Message: Spanning Tree loop guard blocking (Instance :< instance-id >, <interface-id>) Parameters Description: Instance-id: MST instance id. Instance 0 represents for default instance, CIST. Interface_id: The port number which detect the event.	Informational

OSPFv2

Log Description	Severity
Event Description: OSPF interface link state changed. Log Message: 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 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 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.	Notification

Log Message: 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.	
Event Description: One OSPF neighbor state changed from Full to Down. Log Message: 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.	Notification
Event Description: One OSPF neighbor state's dead timer expired. Log Message: 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.	Notification
Event Description: One OSPF virtual neighbor state changed from Loading to Full. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Loading to Full Parameters Description: nbr-id: Neighbor's router ID.	Notification
Event Description: One OSPF virtual neighbor state changed from Full to Down. Log Message: OSPF nbr <nbr-id> on virtual link changed state from Full to Down Parameters Description: nbr-id: Neighbor's router ID.	Notification
Event Description: OSPF router ID was changed. Log Message: OSPF router ID changed to <router-id> Parameters Description: router-id: OSPF router ID.	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: Unit <id>: The unit ID. fan-descr: The FAN ID and position.	Critical
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: Press the factory reset button. Log Message: Unit <unit-id> factory reset button pressed Parameters Description: unitID: The unit ID.	Critical

PoE

Log Description	Severity
Event Description: Total power usage threshold is exceeded. Log Message: Unit <unit-id> usage threshold <percentage> is exceeded Parameters Description: unit-id: The box ID. percentage: Usage threshold.	Warning
Event Description: Total power usage threshold is recovered. Log Message: Unit <unit-id> usage threshold <percentage> is recovered Parameters Description: unit-id: The box ID. percentage: Usage threshold.	Warning
Event Description: PD doesn't reply the ping request. Log Message: PD alive check failed. (Port: <portNum>, PD: <ipaddr>) portNum: The port number. ipaddr: The IP (IPv4/IPv6) address of PD.	Warning

Port Security

Log Description	Severity
Event Description: Address full on a port. Log Message: MAC address <mac-address> 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

Safeguard

Log Description	Severity
Event Description: When the CPU utilization is over the rising threshold, the switch enters exhausted mode, and the syslog will be recorded. Log Message: Unit <unit-id>, Safeguard Engine enters EXHAUSTED mode Parameters Description: unit-id: Unit ID.	Warning
Event Description: When the CPU utilization is lower than the falling threshold, the switch enters normal mode, and the syslog will be recorded. Log Message: Unit <unit-id>, Safeguard Engine enters NORMAL mode Parameters Description: unit-id: 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

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:	Informational

unitID: Box ID. Macaddr: MAC address.	
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
Event Description: Stacking port linkup. A Stacking port will act as a SIO interface or a member of a SIO interface (SIO Trunk). This log entry is only available on projects that stacking port has got a port number indicator on device's panel. Log Message: Stacking port <port> link up Parameters Description: port: Represents the logical port number of a Stacking port.	Critical
Event Description: Stacking port linkdown. A Stacking port will act as a SIO interface or a member of a SIO interface (SIO Trunk). This log entry is only available on projects that stacking port has got a port number indicator on device's panel. Log Message: Stacking port <port> link down Parameters Description: port: Represents the logical port number of a Stacking port.	Critical
Event Description: SIO interface linkup. For SIO Trunk, the first member port link up will trigger this event. Log Message: SIO interface Unit <unitID> <SIOn > link up Parameters Description: unitID: Box ID. SIOn: Represents the SIO interface number. Current Supported SIO interface number should be SIO1 and SIO2.	Critical
Event Description: SIO interface linkdown. For SIO Trunk, the last member port link down will trigger this event. Log Message: SIO interface Unit <unitID> <SIOn > link down Parameters Description: unitID: Box ID. SIOn: Represents the SIO interface number. Current Supported SIO interface number should be SIO1 and SIO2.	Critical

Storm Control

Log Description	Severity
Event Description: Storm occurrence. 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 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 ID on which is error-disabled by storm. 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

System

Log Description	Severity
Event Description: This log will be generated when system warm start. Log Message: [Unit <unitID>,]System warm start Parameters Description: unitID: The unit ID.	Critical
Event Description: This log will be generated when system cold start. Log Message: [Unit <unitID>,]System cold start Parameters Description: unitID: The unit ID.	Critical
Event Description: This log will be generated when system start up. Log Message: [Unit <unitID>,]System started up. Parameters Description: unitID: The unit ID.	Critical

Telnet

Log Description	Severity

Event Description: Successful login through Telnet. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Informational
Event Description: Login failed through Telnet. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Warning
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Informational
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: ipaddr: The IP address of Telnet client. username: the user name that used to login Telnet server.	Informational

Voice VLAN

Log Description	Severity
Event Description: When a new voice device is detected on an interface. Log Message: New voice device detected (<interface-id>, MAC: <mac-address>) Parameters Description: interface-id: Interface name. mac-address: Voice device MAC address.	Informational
Event Description: When an interface which is in auto voice VLAN mode joins the voice VLAN. Log Message: <interface-id> add into voice VLAN <vid> Parameters Description: interface-id: Interface name. vid: VLAN ID.	Informational
Event Description: When an interface leaves the voice VLAN and at the same time, no voice device is detected in the aging interval for that interface, the log message will be sent. Log Message: <interface-id> remove from voice VLAN <vid> Parameters Description: interface-id: Interface name. vid: VLAN ID.	Informational

VRRP Debug

Log Description	Severity
Event Description: One virtual router state becomes Master. Log Message: VR <vr-id> at interface <intf-name> switch to Master	Informational

Parameters Description: vr-id: VRRP virtual router ID. intf-name: Interface name on which virtual router is based.	
Event Description: One virtual router state becomes Backup. Log Message: 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: 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: 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: 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: 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: 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: 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: Added a virtual MAC <vrrp-mac-addr> into L2 table Parameters Description: vrrp-mac-addr: VRRP virtual MAC address.	Notification

Event Description: A virtual MAC address is deleted from switch L2 table. Log Message: Deleted a virtual MAC <vrrp-mac-addr> from L2 table Parameters Description: vrrp-mac-addr: VRRP virtual MAC address.	Notification
Event Description: A virtual MAC address is adding into switch L3 table. Log Message: 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.	Notification
Event Description: A virtual MAC address is deleting from switch L3 table. Log Message: 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.	Notification
Event Description: Failed when adding a virtual MAC into switch chip L2 table. Log Message: 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: 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 behavior.	Error
Event Description: Failed when adding a virtual MAC into switch L3 table. The L3 table is full. Log Message: 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: 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: 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. mac-intf: interface id on which VRRP virtual MAC address is based.	Error
Event Description: Failed when adding a virtual MAC into switch L3 table. The box where the MAC is learned from is invalid.	Error

Log Message: 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.	
Event Description: Failed when adding a virtual MAC into switch chip's L3 table. Log Message: 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: 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. ipaddr: The IP address of HTTP client.	Informational
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.	Informational

ipaddr: The IP address of SSL client.	
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-Auth

Log Description	Severity
Event Description: When a host has passed the authentication. Log Message: Web-Authentication host login success (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: Username: The host username. IP: The host IP 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: When a host fail to pass the authentication. Log Message: Web-Authentication host login fail (Username: <string>, IP: <ipaddr | ipv6address>, MAC: <mac-address>, <interface-id>, VID: <vlan-id>) Parameters Description: Username: The host username. IP: The host IP 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
Event Description: when the authorized user number on the whole device has reached the maximum user limit. Log Message: Web-Authentication enters stop learning state	Warning
Event Description: when the authorized user number on the whole device is below the maximum user limit in a time interval. Log Message: Web-Authentication recovers from stop learning state	Warning

ZTP Table

Log Description	Severity

Event Description: This message means that ZTP Firmware upgraded successfully. Log Message: The downloaded firmware was successfully executed by ZTP update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: TFTP Server IP address.	Informational
Event Description: This message means that ZTP Firmware upgraded unsuccessfully. Log Message: The downloaded firmware was not successfully executed by ZTP update (TFTP Server IP: <ipaddr>) Parameters Description: ipaddr: TFTP Server IP address.	Informational

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

802.1X

Trap Name	Description	OID
dDot1xExtLoggedSuccess	The trap is sent when a host has successfully logged in (passed 802.1X authentication). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName	1.3.6.1.4.1.17 1.14.30.0.1
dDot1xExtLoggedFail	The trap is sent when a host failed to pass 802.1X authentication (login failed). Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan (4) dnaSessionAuthUserName (5) dDot1xExtNotifyFailReason	1.3.6.1.4.1.17 1.14.30.0.2

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

BPDU Protection

Trap Name	Description	OID
dBpduProtectionAttackOccur	This trap is sent when the BPDU attack happened on an interface. Binding objects: (1) ifIndex (2) dBpduProtectionIfCfgMode	1.3.6.1.4.1.17 1.14.47.0.1
dBpduProtectionAttackRecover	This trap is sent when the BPDU attack recovered on an interface. Binding objects: (1) ifIndex	1.3.6.1.4.1.17 1.14.47.0.2

DDM

Trap Name	Description	OID
dDdmAlarmTrap	A notification is generated when an abnormal alarm situation occurs or recovers from an abnormal alarm situation to normal status. Only when the current value > low warning or current value < high warning will send recover trap. Binding objects: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.1
dDdmWarningTrap	A notification is generated when an abnormal warning situation occurs or recovers from an abnormal warning situation to normal status. Binding objects: (1) dDdmNotifyInfoIfIndex, (2) dDdmNotifyInfoComponent (3) dDdmNotifyInfoAbnormalLevel (4) dDdmNotifyInfoThresholdExceedOrRecover	1.3.6.1.4.1.17 1.14.72.0.2

DHCP Server Screen Prevention

Trap Name	Description	OID
dDhcpFilterAttackDetected	When DHCP Server Screen is enabled, if the switch received the forge DHCP Server packet, the switch will trap the event if any attacking packet is received. Binding objects: (1) dDhcpFilterLogBufServerIpAddr (2) dDhcpFilterLogBufClientMacAddr (3) dDhcpFilterLogBufferVlanId (4) dDhcpFilterLogBufferOccurTime	1.3.6.1.4.1.17 1.14.133.0.1

DoS Prevention

Trap Name	Description	OID
dDosPreveAttackDetectedPacket	The trap is sent when detect DOS attack. Binding objects: (1) dDoSPrevCtrlAttackType (2) dDosPrevNotiInfoDropIpAddr (3) dDosPrevNotiInfoDropPortNumber	1.3.6.1.4.1.17 1.14.59.0.2

ErrDisable

Trap Name	Description	OID
dErrDisNotifyPortDisabledAssert	The trap is sent when a port enters into error disabled state.	1.3.6.1.4.1.17 1.14.45.0.1

	Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	
dErrDisNotifyPortDisabledClear	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) dErrDisNotifyInfoPortIfIndex (2) dErrDisNotifyInfoReasonID	1.3.6.1.4.1.17 1.14.45.0.2

General Management

Trap Name	Description	OID
dGenMgmtLoginFail	This trap is sent when the user login failed to the switch. Binding objects: (1) dGenMgmtNotifyInfoLoginType (2) dGenMgmtNotifyInfoUserName	1.3.6.1.4.1.17 1.14.165.0.1

Gratuitous ARP

Trap Name	Description	OID
agentGratuitousARPTrap	The trap is sent when IP address conflicted. Binding objects: (1) ipaddr (2) macaddr (3) portNumber (4) agentGratuitousARPInterfaceName	1.3.6.1.4.1.17 1.14.75.0.1

IP-MAC-Port Binding

Trap Name	Description	OID
dImpbViolationTrap	The address violation notification is generated when IP-MAC-Port Binding address violation is detected. Binding objects: (1) ifIndex (2) dImpbViolationIpAddrType (3) dImpbViolationIpAddress (4) dImpbViolationMacAddress (5) dImpbViolationVlan	1.3.6.1.4.1.17 1.14.22.0.1

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	1.3.6.1.6.3.1.1 .5.4

	notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	
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) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.3

LBD

Trap Name	Description	OID
swPortLoopOccurred	The trap is sent when a port loop occurs. Binding objects: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.1
swPortLoopRestart	The trap is sent when a port loop restarts after the interval time. Binding objects: (1) swLoopDetectPortIndex	1.3.6.1.4.1.17 1.14.46.0.2
swVlanLoopOccurred	The trap is sent when a port loop occurs under LBD VLAN-based mode. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.3
swVlanLoopRestart	The trap is sent when a port loop restarts under LBD VLAN-based mode after the interval time. Binding objects: (1) swLoopDetectPortIndex (2) swVlanLoopDetectVID	1.3.6.1.4.1.17 1.14.46.0.4

LLDP-MED

Trap Name	Description	OID
lldpRemTablesChange	A lldpRemTablesChange notification is sent when the value of lldpStatsRemTableLastChangeTime changes. Binding objects: (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 objects: (1) lldpRemChassisIdSubtype (2) lldpRemChassisId (3) lldpXMedRemDeviceClass	1.0.8808.1.1.2.1.5.4795.0.1

MAC-based Access Control

Trap Name	Description	OID
dMacAuthLoggedSuccess	The trap is sent when a MAC-based Access Control host is successfully logged in. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.1
dMacAuthLoggedFail	The trap is sent when a MAC-based Access Control host login fails. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.2
dMacAuthLoggedAgesOut	The trap is sent when a MAC-based Access Control host ages out. Binding objects: (1) ifIndex (2) dnaSessionClientMacAddress (3) dnaSessionAuthVlan	1.3.6.1.4.1.171.14.153.0.3

MAC Notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicate the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfo	1.3.6.1.4.1.171.14.3.0.1
dL2FdbMacNotificationWithVID	This trap indicate the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.171.14.3.0.2

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	1.3.6.1.2.1.17.0.1

	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.	
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 of this trap is optional.	1.3.6.1.2.1.17.0.2

Peripheral

Trap Name	Description	OID
dEntityExtFanStatusChg	The commander switch will send this notification when a fan fails (dEntityExtEnvFanStatus is 'fault') or recovers (dEntityExtEnvFanStatus is 'ok'). Binding objects: (1) dEntityExtEnvFanUnitId (2) dEntityExtEnvFanIndex (3) dEntityExtEnvFanStatus	1.3.6.1.4.1.171.14.5.0.1
dEntityExtThermalStatusChg	The commander switch will send this notification when a thermal alarms (dEntityExtEnvTempStatus is 'abnormal') or recover(dEntityExtEnvTempStatus is 'ok'). Binding objects: (1) dEntityExtEnvTempUnitId (2) dEntityExtEnvTempIndex (3) dEntityExtEnvTempStatus	1.3.6.1.4.1.171.14.5.0.2
dEntityExtPowerStatusChg	The commander switch will send this notification when a power module fails, recovers or is removed. Binding objects: (1) dEntityExtEnvPowerUnitId (2) dEntityExtEnvPowerIndex (3) dEntityExtEnvPowerStatus	1.3.6.1.4.1.171.14.5.0.3
dEntityExtFactoryResetButton	Press factory reset button notification. Binding objects: (1) dEntityExtUnitIndex	1.3.6.1.4.1.171.14.5.0.5

PIM6-SM

Trap Name	Description	OID
pimNeighborLoss	A pimNeighborLoss notification signifies the loss of an adjacency with a neighbor. This notification should be generated when the neighbor timer expires, and the router has no other neighbor on the same interface with the same IP version and a lower IP address than itself. This notification is generated whenever the counter pimNeighborLossCount is incremented, subject to the rate limit specified by pimNieghborLossNotificationsPeriod. Binding objects:	1.3.6.1.2.1.157.0.1

	(1) pimNeighborUpTime	
pimInvalidRegister	A pimInvalidRegister notification signifies that an invalid PIM Register message was received by this device. This notification is generated whenever the counter pimInvalidRegisterMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidRegisterNotificationPeriod. Binding objects: (1) pimGroupMappingPimMode (2) pimInvalidRegisterAddressType (3) pimInvalidRegisterOrigin (4) pimInvalidRegisterGroup (5) pimInvalidRegisterRp	1.3.6.1.2.1.157.0.2
pimInvalidJoinPrune	A pimInvalidJoinPrune notification signifies that an invalid PIM Join/Prune message was received by this device. This notification is generated whenever the counter pimInvalidJoinPruneMsgsRcvd is incremented, subject to the rate limit specified by pimInvalidJoinPruneNotificationPeriod. Binding objects: (1) pimGroupMappingPimMode (2) pimInvalidJoinPruneAddressType (3) pimInvalidJoinPruneOrigin (4) pimInvalidJoinPruneGroup (5) pimInvalidJoinPruneRp (6) pimNeighborUpTime	1.3.6.1.2.1.157.0.3
pimRPMappingChage	A pimRPMappingChange notification signifies a change to the active RP mapping on this device. This notification is generated whenever the counter pimRPMappingChangeCount is incremented, subject to the rate limit specified by pimRPMappingChangeNotificationPeriod. Binding objects: (1) pimGroupMappingPimMode (2) pimGroupMappingPrecedence	1.3.6.1.2.1.157.0.4
pimInterfaceElection	A pimInterfaceElection notification signifies that a new DR or DF has been elected on a network. This notification is generated whenever the counter pimInterfaceElectionWinCount is incremented, subject to the rate limit specified by pimInterfaceElectionNotificationPeriod. Binding objects: (1) pimInterfaceAddressType (2) pimInterfaceAddress	1.3.6.1.2.1.157.0.5

PoE

Trap Name	Description	OID
pethMainPowerUsageOnNotification	This trap indicates PSE Threshold usage indication is on, the usage power is above the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance.	1.3.6.1.2.1.105.0.2

	Binding objects: (1) pethMainPseConsumptionPower	
pethMainPowerUsageOffNotification	This trap indicates PSE Threshold usage indication is off, The usage power is below the threshold. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.105.0.3
dPoeIfPowerDeniedNotification	This Notification indicates if PSE state diagram enters the state POWER_DENIED. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortPowerDeniedCounter	1.3.6.1.4.1.171.14.24.0.1
dPoeIfPowerOverLoadNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_OVER. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortOverLoadCounter	1.3.6.1.4.1.171.14.24.0.2
dPoeIfPowerShortCircuitNotification	This trap indicates if PSE state diagram enters the state ERROR_DELAY_SHORT. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethPsePortShortCounter	1.3.6.1.4.1.171.14.24.0.3
dPoeIfPdAliveFailOccurNotification	This trap indicates if the PD device has the stop working or no response problem. At least 500 msec must elapse between notifications being emitted by the same object instance. Binding objects: (1) pethMainPseGroupIndex (2) pethPsePortIndex (3) dPoeIfPdAliveCfgPdIpType (4) dPoeIfPdAliveCfgPdIpAddr	1.3.6.1.4.1.171.14.24.0.4

Port

Trap Name	Description	OID
linkup	A notification is generated when port linkup. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.4
linkDown	A notification is generated when port link down. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1.5.3

Port Security

Trap Name	Description	OID
dPortSecMacAddrViolation	When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out. Binding objects: (1) ifIndex (2) dPortSecIfCurrentStatus (3) dPortSecIfViolationMacAddress	1.3.6.1.4.1.17 1.14.8.0.1

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

Safeguard

Trap Name	Description	OID
dSafeguardChgToExhausted	This trap indicates System change operation mode from normal to exhaust. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 1
dSafeguardChgToNormal	This trap indicates system change operation mode from exhausted to normal. Binding objects: (1) dSafeguardEngineCurrentMode	1.3.6.1.4.1.17 1.14.19.1.1.0. 2

SIM

Trap Name	Description	OID

swSingleIPMSColdStart	The commander switch will send this notification when its member generates a cold start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.11
swSingleIPMSWarmStart	The commander switch will send this notification when its member generates a warm start notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.12
swSingleIPMSLinkDown	The commander switch will send this notification when its member generates a link down notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.13
swSingleIPMSLinkUp	The commander switch will send this notification when its member generates a link up notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr (3) ifIndex	1.3.6.1.4.1.17 1.12.8.6.0.14
swSingleIPMSAuthFail	The commander switch will send this notification when its member generates an authentication failure notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.15
swSingleIPMSnewRoot	The commander switch will send this notification when its member generates a new root notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.16
swSingleIPMSTopologyChange	The commander switch will send this notification when its member generates a topology change notification. Binding objects: (1) swSingleIPMSID (2) swSingleIPMSMacAddr	1.3.6.1.4.1.17 1.12.8.6.0.17

Stacking

Trap Name	Description	OID
dStackInsertNotification	Unit Hot Insert notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.1
dStackRemoveNotification	Unit Hot Remove notification. Binding objects: (1) dStackNotifyInfoBoxId (2) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.2

dStackFailureNotification	Unit Failure notification. Binding objects: (1) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.3
dStackTPChangeNotification	The stacking topology change notification. Binding objects: (1) dStackNotifyInfoTopologyType (2) dStackNotifyInfoBoxId (3) dStackInfoMacAddr	1.3.6.1.4.1.17 1.14.9.0.4
dStackRoleChangeNotification	The stacking unit role change notification. Binding objects: (1) dStackNotifyInfoRoleChangeType (2) dStackNotifyInfoBoxId	1.3.6.1.4.1.17 1.14.9.0.5

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

Storm Control

Trap Name	Description	OID
dStormCtrlOccurred	This trap is sent when dStormCtrlNotifyEnable is 'stormOccurred' or 'both' and a storm is detected. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.1
dStormCtrlStormCleared	This trap is sent when dStormCtrlNotifyEnable is 'stormCleared' or 'both' and a storm is cleared. Binding objects: (1) ifIndex (2) dStormCtrlNotifyTrafficType	1.3.6.1.4.1.17 1.14.25.0.2

System File

Trap Name	Description	OID
dsfUploadImage	The notification is sent when the user uploads image file successfully.	1.3.6.1.4.1.17 1.14.14.0.1
dsfDownloadImage	The notification is sent when the user downloads image file successfully.	1.3.6.1.4.1.17 1.14.14.0.2
dsfUploadCfg	The notification is sent when the user uploads configuration file successfully.	1.3.6.1.4.1.17 1.14.14.0.3

dsfDownloadCfg	The notification is sent when the user downloads configuration file successfully.	1.3.6.1.4.1.17 1.14.14.0.4
dsfSaveCfg	The notification is sent when the user saves configuration file successfully.	1.3.6.1.4.1.17 1.14.14.0.5

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

Web-Authentication

Trap Name	Description	OID
swWACLoggedSuccess	The trap is sent when a WAC client pass the authentication. Binding objects: (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.17 1.14.154.0.1
swWACLoggedFail	The trap is sent when a WAC client failed to pass the authentication. Binding objects: (1) swWACAuthStatePort (2) swWACAuthStateOriginalVid (3) swWACAuthStateMACAddr (4) swWACAuthUserName (5) swWACClientAddrType (6) swWACClientAddress	1.3.6.1.4.1.17 1.14.154.0.2

ZTP

Trap Name	Description	OID
swResetButtonPressedTrap	This object indicates which function is triggered by pressing Reset_Button.	1.3.6.1.4.1.17 1.12.120.2.0.1

	Binding objects: (1) swResetButtonMode

Appendix D - RADIUS Attributes Assignment

The RADIUS Attributes Assignment on the Switch 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.

```
 0                   1                   2                   3
 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|      Type     |    Length     |     Tag       |   String...
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

The table below shows the definition of Tag field (different with RFC 2868):

Tag field value	String field format
0x01	VLAN name (ASCII)
0x02	VLAN ID (ASCII)
Others (0x00, 0x03 ~ 0x1F, >0x1F)	When the Switch receives the VLAN setting string, it will think it is the VLAN ID first. In other words, the Switch will check all existing VLAN IDs and check if there is one matched. If the Switch can find one matched, it will move to that VLAN. If the Switch cannot find the matched VLAN ID, it will think the VLAN setting string as a “VLAN Name”. Then it will check that it can find out a matched VLAN Name.



NOTE: A tag field of greater than 0x1F is interpreted as the first octet of the following field.

If the user has configured the VLAN attribute of the RADIUS server (for example, VID 3) and the 802.1X, 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.

VSA14 ACL Script

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, MAC-based Access Control, JWAC or WAC authentication 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.

NAS-Filter-Rule (92)

The table below shows the parameters for NAS-Filter-Rule:

RADIUS Tunnel Attribute	Description	Value	Usage
NAS-Filter-Rule	This attribute indicates the filter rules to be applied for the user.	A string (concatenating the individual filter rules, separated by a NULL (0x00) octet)	Required

Filter Rule Format

Use the permit command to add a permit entry. Use the deny command to add a deny entry.

{permit | deny} in tcp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***TCP-PORT-RANGE***]**

{permit | deny} in udp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***UDP-PORT-RANGE***]**

{permit | deny} in icmp from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***} [***ICMP-TYPE***]**

{permit | deny} in ip from any to {any | *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

{permit | deny} in *IP-PROT-VALUE* **from any to {any |** *DST-IP-ADDR* **|** *DST-IP-NET-ADDR* **|** *DST-IPV6-ADDR* **|** *DST-IPV6-NET-ADDR***}**

Filter Rule Format

any	Specifies any source IP address or any destination IP address to be configured.
DST-IP-ADDR	Specifies a specific destination host IP address.
DST-IP-NET-ADDR	Specifies a group of destination IP addresses with a mask width of the form 1.2.3.4/24.
DST-IPV6-ADDR	Specifies a specific destination host IPv6 address.
DST-IPV6-NET-ADDR	Specifies a group of destination IPv6 network of the form 2000::1/64.
tcp, udp, icmp	Specifies Layer 4 protocols.
ip	Specifies that any protocol will match.
IP-PROT-VALUE	Specifies the IP protocol value. The valid value is from 0 to 255.
TCP-PORT-RANGE	(Optional) Specifies to match TCP port or port range. The form is like 22-23, 80.
UDP-PORT-RANGE	(Optional) Specifies to match UDP port or port range. The form is like 56, 67-68.
ICMP-TYPE	(Optional) Specifies the ICMP message type. The valid number for the message type is from 0 to 255.

Example

This example shows how to deny host's telnet service on the RADIUS server.

```
Nas-filter-Rule="deny in tcp from any to any 23"
Nas-filter-Rule+="permit in ip from any to any"
```

This example shows how to limit host to access a group of IP address on the RADIUS server.

```
Nas-filter-Rule="permit in ip from any to 10.10.10.1/24"
Nas-filter-Rule+="permit in ip from any to fe80::d1:1/64"
```

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	IPv6 filter rule. Used to accept IPv6 address related inputs.	This attribute indicates either of the following IP modes for NAS-Filter-Rule 1=Forward IPv4 and IPv6 traffic 2=Forward IPv4-only traffic (drop any IPv6 traffic) If this attribute is not assigned by RADIUS server, forward IPv4-only traffic, any IPv6 packet will be dropped.	Required

NOTE: If both proprietary ACL script (VSA14) and standard NAS-Filter-Rule (92) are assigned at the same time, NAS-Filter-Rule (92) will take effect, and VSA14 will be ignored.

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

Appendix F - ERPS Information

Only hardware-based ERPS supports the Fast Link Drop Interrupt feature with a recovery time of 50 milliseconds in a 16-node ring. The distance must be less than 1200 kilometers.

Model Name	ERPS	Port 1 to 8	Port 9 to 26	Port 27 to 28
DGS-1520-28	Hardware-based	V		V
	Software-based		V	

Model Name	ERPS	Port 1 to 4	Port 5 to 26	Port 27 to 28
DGS-1520-28MP	Hardware-based	V		V
	Software-based		V	

Model Name	ERPS	Port 1 to 8	Port 9 to 24	Port 25 to 32	Port 33 to 50	Port 51 to 52
DGS-1520-52	Hardware-based	V		V		V
	Software-based		V		V	

Model Name	ERPS	Port 1 to 8	Port 9 to 24	Port 25 to 28	Port 29 to 50	Port 51 to 52
DGS-1520-52MP	Hardware-based	V		V		V
	Software-based		V		V	

Appendix G - Stacking Information

The following stacking topologies are supported on the Switch:

- **Duplex Chain** - This topology stacks switches together in a chain-link format. Using this method, data transfer is only possible in one direction. If there is a break in the chain, data transfer will be affected.
- **Duplex Ring** - This topology stacks switches in a ring or circle format where data can be transferred in two directions. It is very resilient because if there is a break in the ring, data can still be transferred through the stacking cables between switches in the stack using the alternate path.

In the following diagram, an even number of switches (for example 4 switches) are stacked in the duplex chain topology using the **2-port** stacking configuration through the two 10GBASE-T ports.

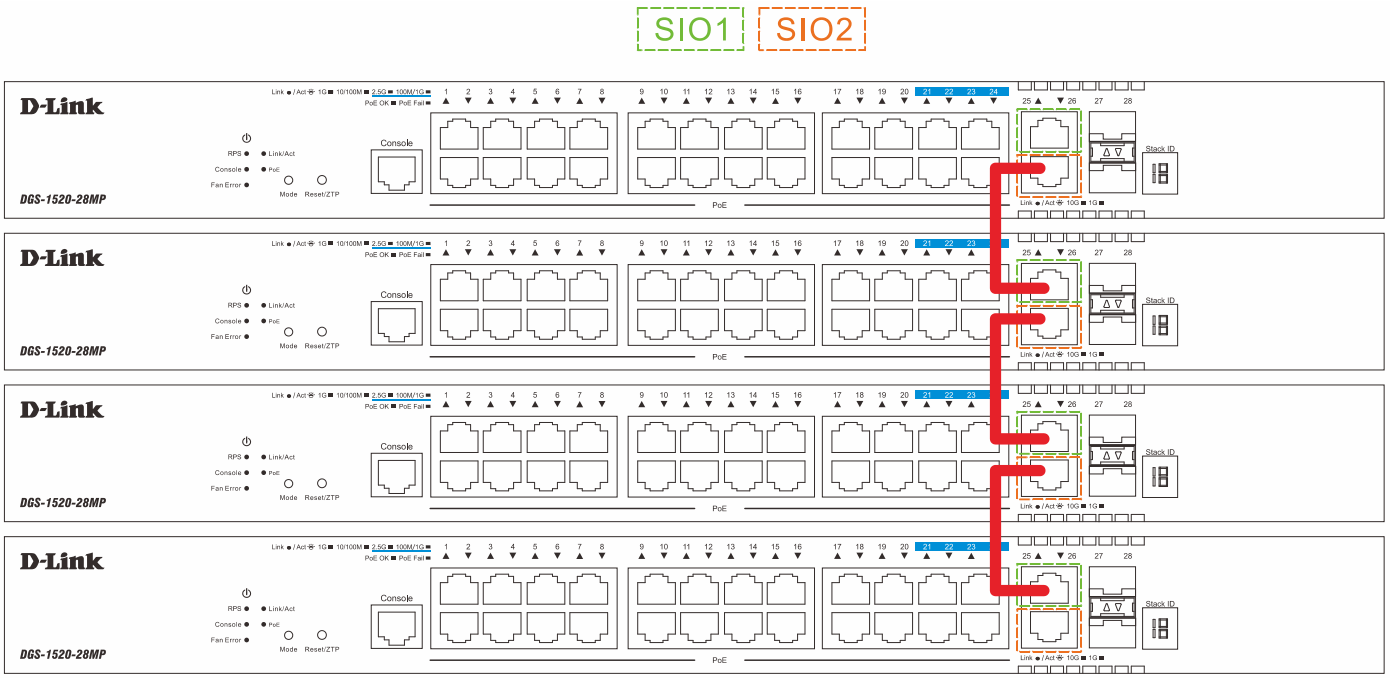


Figure 1 - Duplex Chain Stacking Topology (Even, 2-port)

In the following diagram, an even number of switches (for example 4 switches) are stacked in the duplex ring topology using the **2-port** stacking configuration through the two 10GBASE-T ports.

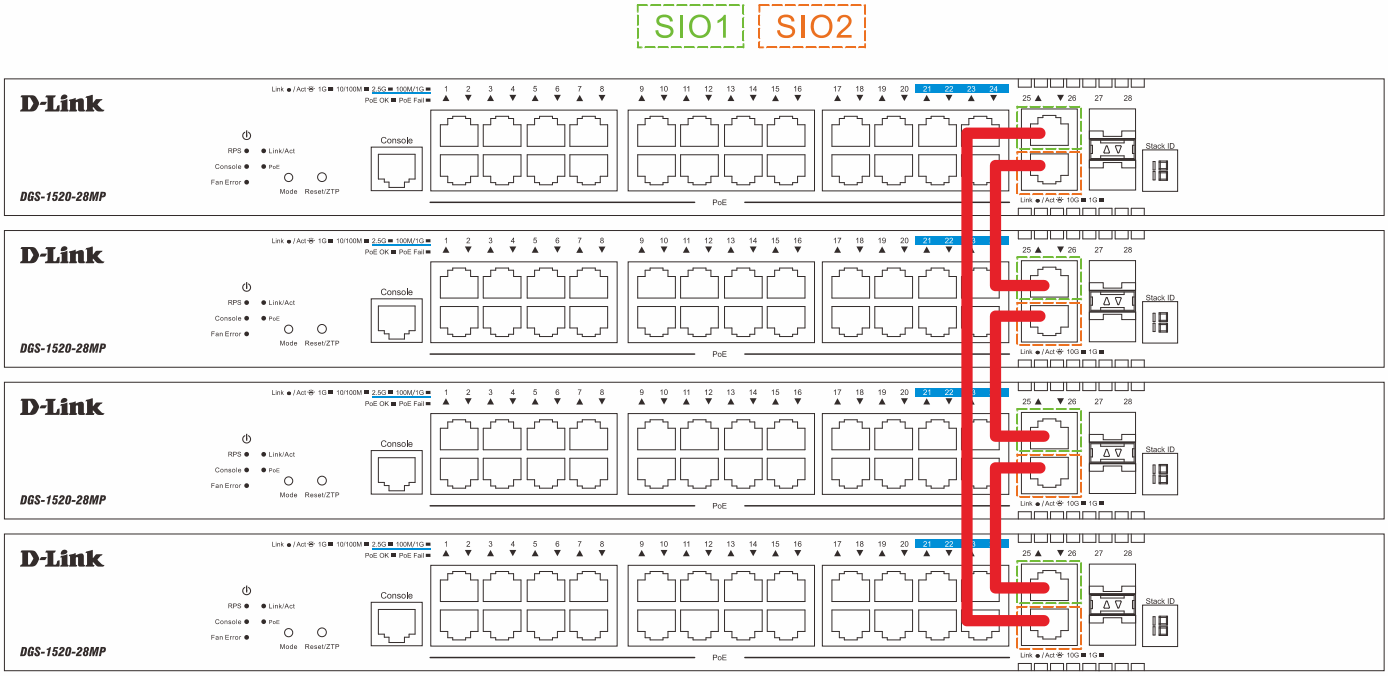


Figure 2 - Duplex Ring Stacking Topology (Even, 2-port)

In the following diagram, an even number of switches (for example 4 switches) are stacked in the duplex chain topology using the **4-port** stacking configuration.

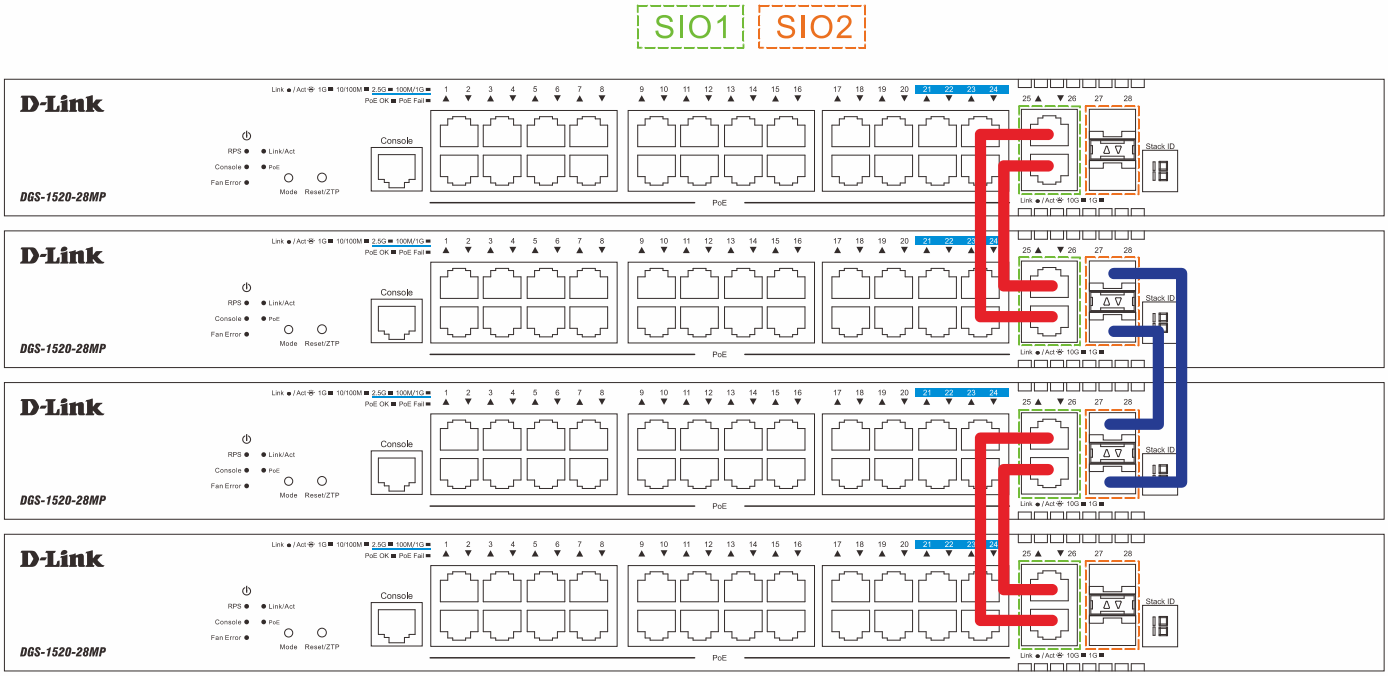


Figure 3 - Duplex Chain Stacking Topology (Even, 4-port)

In the following diagram, an even number of switches (for example 4 switches) are stacked in the **duplex ring** topology using the **4-port** stacking configuration.

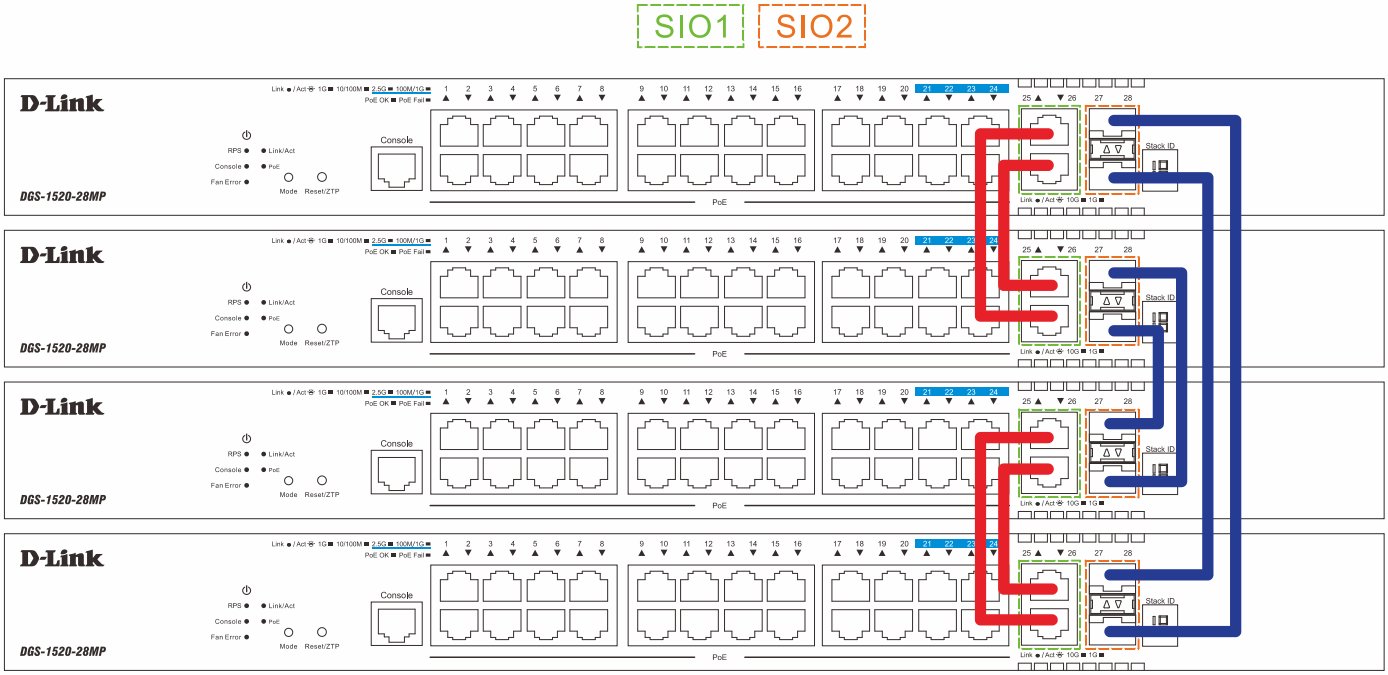


Figure 4 - Duplex Ring Stacking Topology (Even, 4-port)

In the following diagram, an odd number of switches (for example 3 switches) are stacked in the **duplex chain** topology using the **4-port** stacking configuration.

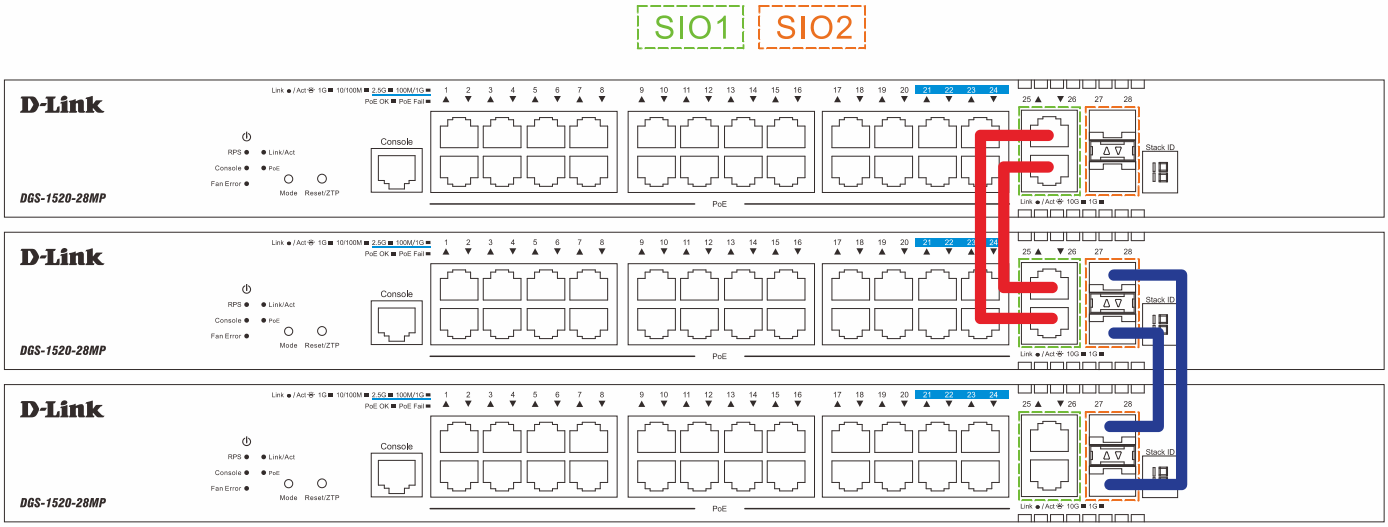


Figure 5 - Duplex Chain Stacking Topology (Odd, 4-port)

In the following diagram, an odd number of switches (for example 3 switches) are stacked in the **duplex ring** topology using the **4-port** stacking configuration. The topology is not supported on switches in this series.

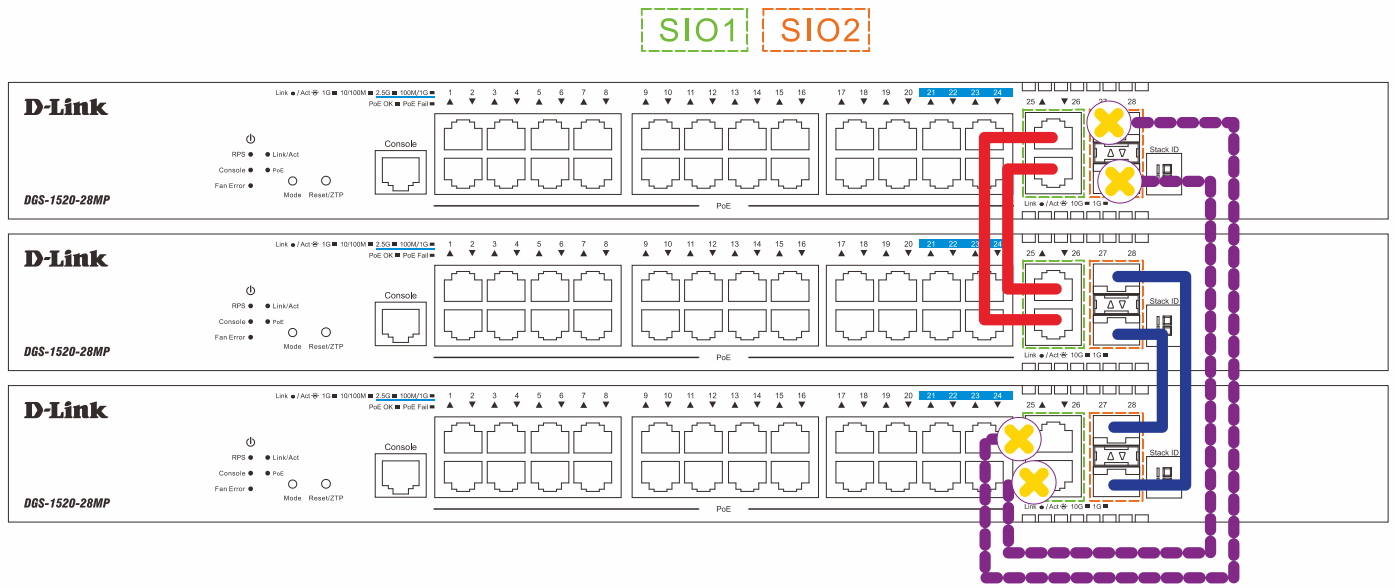


Figure 6 Duplex Ring Stacking Topology (Odd, 4-port)