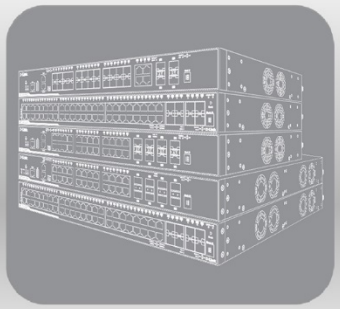
D-Link
Building Networks for People



CLI Reference Guide

Product Model: DGS-3630 Series

Layer 3 Stackable Managed Switch

Release 2.25 (OpenFlow)

Table of Contents

1. Introduction

This manual's command descriptions are based on the software release **2.25**, running in the **OpenFlow Mode**. The commands listed here are the subset of commands that are supported by the DGS-3630 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-3630 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-3630 Series Hardware Installation Guide*
- *DGS-3630 Series Web UI Reference Guide (OpenFlow)*

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-3630-28TC switch in the DGS-3630 Series.

Notes, Notices, and Cautions

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

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

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

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

Command Descriptions

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

- **Description** - This is a short and concise statement describing the 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.
VLAN Interface Configuration Mode	For applying VLAN 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 or out-of-band 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

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

Observe the following example.

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

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

- Starting in the User EXEC Mode, we enter the **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 admin password admin** command creates a user account with the username of admin and a password of admin.

- The **username admin 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-3630-28PC Gigabit Ethernet Switch

                                Command Line Interface
                               Firmware: Build 2.25.013
                 Copyright(C) 2021 D-Link Corporation. All rights reserved.

User Verification Access
Username:admin
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'll enter the Global Configuration Mode and then enter the Interface Configuration Mode, using the notation **1/0/1**. After entering the Interface Configuration Mode for port 1, we'll change the speed to 1 Gbps, using the **speed 1000** command.

```
Switch# configure terminal
Switch(config)# interface 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, then this parameter is irrelevant. The Open Slot's ID is the ID of the module plugged into the open module slot of the Switch. The DGS-3630 Series switch doesn't 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
!
openflow global enable
!
!
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 : 1341 bytes


line console
line telnet
line ssh
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
interface ethernet 1/0/12
interface ethernet 1/0/13
interface ethernet 1/0/14
interface ethernet 1/0/15
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  reset

Switch#re
```

The following example shows how to use the **command syntax** help to display the next argument of a partially complete **reboot** 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#reboot ?
  force_agree  Forcibly reboot without prompting for user input
  schedule     Schedule to restart
  <cr>

Switch#
```

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 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 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, there is no login method configured for the **console** line.

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

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

Command Mode

Line Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

- When login is disabled, the user can enter the line at Level 1.
- When the **by password** option is selected, after inputting the same password as the **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.

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         29C/0~45C
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) Specifies 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         Model Descr                              Model Name
----  ---------------------------------------  ----------------------------
 1     24P PoE 10/100/1000 with 4P Combo 4P SFP+    DGS-3630-28PC

Unit         Serial-Number                Status        Up Time
----  --------------------------------  ---------  -----------------
 1     DGS3630-28PC1                     ok            0DT1H13M2S

Unit   Memory     Total       Used        Free
----  --------  ----------  ----------  ----------
 1     DRAM     1048576 K    419338 K    629238 K
 1     FLASH    1039872 K     54278 K    985594 K

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:
9  Apr 2021  14:57:12 - 9  Apr 2021  14:42:12  : 14  %
9  Apr 2021  14:42:12 - 9  Apr 2021  14:27:12  : 14  %
9  Apr 2021  14:27:12 - 9  Apr 2021  14:12:12  : 14  %
9  Apr 2021  14:12:12 - 9  Apr 2021  13:57:12  : 14  %
9  Apr 2021  13:57:12 - 9  Apr 2021  13:42:12  : 14  %

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: F0-7D-68-30-36-00

Unit ID    Module Name                    Versions
-------  ---------------------------  --------------------
   1      DGS-3630-28PC                H/W:A1
                                       Bootloader:2.10.001
                                       Runtime:2.25.013


Switch#
```

2-16 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.
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)#
```

2-17 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 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.

Historical memory utilization information only displays DRAM memory information.

Example

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

```
Switch#show memory utilization


Unit   Memory     Total       Used        Free
----  --------  ----------  ----------  ----------
 1     DRAM     1048576 K    377297 K    671279 K
 1     FLASH    1039872 K     45812 K    994060 K

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:
10 Apr 2021  14:25:28 - 10 Apr 2021  14:10:28  : 39  %
10 Apr 2021  14:10:28 - 10 Apr 2021  13:55:28  : 39  %
10 Apr 2021  13:55:28 - 10 Apr 2021  13:40:28  : 39  %
10 Apr 2021  13:40:28 - 10 Apr 2021  13:25:28  : 39  %
10 Apr 2021  13:25:28 - 10 Apr 2021  13:10:28  : 39  %

Switch#
```

2-18 console-usb-timeout (Hybrid Mode Only)

This command is used to configure the console timeout value after which the mini-USB console port will switch access to the RJ45 console port due to inactivity. Use the **no** form of this command to set the mini-USB console timeout to never.

console-usb-timeout *MINUTES*

no console-usb-timeout

Parameters

MINUTES	Specifies the mini-USB console port timeout in minute. The value is from 1 to 240.

Default

By default, the mini-USB console port never times out.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to configure the mini-USB console port timeout in minutes. After the mini-USB console port is deactivated due to timeout, it cannot be reactivated through Web or CLI until the mini-USB console cable is removed from the port and then re-inserted.

Example

This example shows how to configure the mini-USB console port timeout to 10 minutes.

```
Switch#configure terminal
Switch(config)#console-usb-timeout 10
Switch(config)#
```

2-19 console-usb (Hybrid Mode Only)

This command is used to configure the console media type to use mini-USB first. Use the **no** form of this command to immediately deactivate the connected mini-USB console.

console-usb

no console-usb

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 configure the console media type priority.

When the **console-usb** command is configured, the console media type uses mini-USB first. If the mini-USB console port is not connected, RJ45 console will be used.

When the **no console-usb** command is configured, the mini-USB console is deactivated, and the console media type always uses RJ45.

Example

This example shows how to enable the mini-USB console.

```
Switch#configure terminal
Switch(config)#console-usb
Switch(config)#
```

2-20 privilege (Hybrid Mode Only)

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)#
```

2-21 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. Access Management Commands

3-1 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, then the login banner contents can be typed. The delimiting character need to be input then press enter to complete the type. To configure the login banner contents to default, use **no** banner login command in global configuration mode.

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

Example

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

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

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

```
Switch#configure terminal
Switch(config)#banner login #
Enter TEXT message.  End with the character '#'.
Enter Command Line Interface
#
Switch(config)#
```

3-2 do

This command is used to execute commands orgininally 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 orgininally 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.

Example

This example shows how to excute the **show privilege** command in the global configuration mode.

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

Current privilege level is 15

Switch(config)#
```

3-3 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** – encode the SNMP server name. **%s** – space **%%** - 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)#
```

3-4 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 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

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)#
```

3-5 ip http server (Hybrid Mode Only)

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

This command enables the HTTP server function. The HTTPs access interface is separately controlled by SSL commands.

Example

This example shows how to enable the HTTP server.

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

3-6 ip http secure-server (Hybrid Mode Only)

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

ip http secure-server

no ip http secure-server

Parameters

None.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command enables the HTTPS server function.

Example

This example shows how to enable the HTTPS server function.

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

3-7 ip http secure-server ssl-service-policy

This command is used to to specify which SSL service policy is used for HTTPS. Use the **no** form of this command to clear the SSL service policy.

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

no ip http secure-server

Parameters

POLICY-NAME	Specifies the SSL service policy name.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to specify the SSL service policy for HTTPS. This command can only be used when an SSL service policy is declared using the **ssl-service-policy** command.

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)#
```

3-8 ip http service-port (Hybrid Mode Only)

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)#
```

3-9 ip http timeout-policy idle (Hybrid Mode Only)

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)#
```

3-10 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)#
```

3-11 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)#
```

3-12 line

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

line {console | telnet | ssh}

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The line command is used to enter the Line Configuration Mode.

Example

This example shows how to enter the Line Configuration Mode for the SSH terminal line and configures its session timeout value.

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

3-13 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)#
```

3-14 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.
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)#
```

3-15 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: 9600 bps

Switch#
```

3-16 show ip telnet server (Hybrid Mode Only)

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#
```

3-17 show ip http server (Hybrid Mode Only)

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 :  Enable
Switch#
```

3-18 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#
```

3-19 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#
```

3-20 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

This command displays 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#
```

3-21 telnet (Hybrid Mode Only)

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

telnet [*IP-ADDRESS* **|** *IPV6-ADDRESS***] [***TCP-PORT***]**

Parameters

IP-ADDRESS	Specifies the IPv4 address of the host.
IPV6-ADDRESS	Specifies the IPv6 address of the host.
TCP-PORT	Specifies the TCP port number. TCP ports are numbered between 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-3630-28TC management interface which allows a user to login.

```
Switch# telnet 10.90.90.91

                     DGS-3630-28TC Gigabit Ethernet Switch

                           Command Line Interface
                          Firmware: Build 2.25.013
          Copyright(C) 2021 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

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

```
Switch#telnet 10.90.90.91

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

Switch# telnet 10.90.90.91 3500

                     DGS-3630-28TC Gigabit Ethernet Switch

                           Command Line Interface
                          Firmware: Build 2.25.013
          Copyright(C) 2021 D-Link Corporation. All rights reserved.

Password required, but none set

Switch#
```

3-22 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 default length** command will set the default value but it doesn't affect the current session. The newly created, saved session terminal length will use the default value. Use 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, then the display will stop after every 50 lines. The terminal length is used to set the number of lines displayed on the current terminal screen. This command also applies to Telnet and SSH sessions. Valid entries are from 0 to 512. The default is 24 lines. A selection of 0's instructs the Switch to scroll continuously (no pausing).

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

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

Example

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

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

3-23 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)#
```

3-24 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)#
```

3-25 terminal width

The command is used to set the number of character columns on the terminal screen for the current session line. The **terminal width** command will only affect the current session. The **terminal width default** command will set the default value, but it doesn't affect any current sessions. 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# show terminal

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

Switch# terminal width 120
Switch# show terminal

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

Switch #
```

3-26 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.
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, no username-based authentication system is established.

If not specified, use 1.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

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

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

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

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

Example

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

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

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

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

3-27 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)#
```

3-28 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#
```

3-29 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 a 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)#
```

3-30 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)#
```

3-31 outgoing-session-timeout (Hybrid Mode Only)

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)#
```

3-32 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#
```

4. Alias Commands (Hybrid Mode Only)

4-1 alias

This command is used to create an alias for a command. Use the **no** form of this command to delete all aliases or the specified alias, or revert to the default settings.

alias *MODE COMMAND-ALIAS ORIGINAL-COMMAND*

no alias *MODE* **[***COMMAND-ALIAS***]**

Parameters

MODE	Specifies the command mode. Use the **alias ?** command in the Global Configuration mode to see all the available command modes.
COMMAND-ALIAS	Specifies an alias for the command with a maximum of 16 characters. No space is allowed.
ORIGINAL-COMMAND	Specifies the original command with a maximum of 128 characters.

Default

Command Alias	Original Command
h	help
lo	logout
p	ping
s	show

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to create an alias for a command. As explained in the **help** command, entering a partial command followed by a question mark (?) will list the possible command options that will be associated with the partial command. For example, entering the partial command “co?” will list the possible commands **configure**, and **copy**. If an alias was created, it will be preceded with an asterisk (*).For example, entering the partial command “co?” will then list the possible commands ***copy-rs="copy running-config startup-config"**, **configure**, and **copy**. To omit aliases from the output, using the question mark, enter a space before the partial command. For example, “ co?”.

Example

This example shows how to create copy-rs as the alias for the **copy running-config startup-config** command in the EXEC mode.

```
Switch#configure terminal
Switch(config)#alias exec copy-rs copy running-config startup-config
Switch(config)#
```

4-2 show aliases

This command is used to display all the commands that have aliases in the specified mode.

show aliases [*MODE***]**

Parameters

MODE	(Optional) Specifies the command mode.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display all the commands that have aliases in the specified mode. When no optional parameter is specified, all aliases on the system will be displayed.

Example

This example shows how to display alias in the EXEC mode.

```
Switch#show aliases exec
Exec mode aliases:
  h                    help
  lo                   logout
  p                    ping
  s                    show
  copy-rs              copy running-config startup-config

Switch#
```

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

5-1 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)#
```

5-2 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)#
```

5-3 aaa accounting network (Hybrid Mode Only)

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)#
```

5-4 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)#
```

5-5 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)#
```

5-6 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, then the authentication will be performed via the local database.

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

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

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

Example

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

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

5-7 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 that does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

5-8 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 that does not allow spaces.

Default

There is no AAA group server.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

5-9 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)#
```

5-10 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)#
```

5-11 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)#
```

5-12 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. **(Hybrid Mode Only)**
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. **(Hybrid Mode Only)**
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#
```

5-13 ip http authentication aaa login-authentication (Hybrid Mode Only)

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)#
```

5-14 ip http accounting exec (Hybrid Mode Only)

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)#
```

5-15 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)#
```

5-16 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

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)#
```

5-17 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)#
```

5-18 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*

Parameters

IP-ADDRESS	Specifies the IP address of the RADIUS server.
IPV6-ADDRESS	Specifies the IPv6 address of the RADIUS server. **(Hybrid Mode Only)**
auth-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending authentication packets. The range is 0 to 65535. Set the port number to zero if the server host is not for authentication purposes. The default value is 1812.
acct-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending accounting packets. The range is 0 to 65535. Set the port number to zero if the server host is not for accounting purposes. The default value is 1813.
timeout *SECONDS*	Specifies the server time-out value. The range of timeout is between 1 and 255 seconds. If not specified, the default value is 5 seconds.

retransmit *COUNT*	(Optional) Specifies the retransmit times of requests to the server when no response is received. The value is from 0 to 20. Use 0 to disable the retransmission. If not specified, the default value is 2
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)#
```

5-19 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. **(Hybrid Mode Only)**

Default

By default, no server is configured.

Command Mode

RADIUS Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to enter the RADIUS group server configuration mode. Use the **server** command to associate the RADIUS server hosts with the RADIUS server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** 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)#
```

5-20 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.	**(Hybrid Mode Only)**

Default

By default, no host is in the server group.

Command Mode

TACACS+ Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use the **aaa group server tacacs+** command to enter the TACACS+ group server configuration mode. Use the **server** command to associate the TACACS+ server hosts with the TACACS+ server group. The defined server group can be specified as the method list for authentication, or accounting via the **aaa authentication** and **aaa accounting** 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+)#
```

5-21 show aaa

This command is used to display the AAA global state.

show aaa

Parameters

None.

Default

None.

Command Mode

User/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#
```

5-22 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***] [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. **(Hybrid Mode Only)**
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)#
```

5-23 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.

5-24 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.

6. Basic IPv4 Commands

6-1 arp (Hybrid Mode Only)

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)#
```

6-2 arp timeout (Hybrid Mode Only)

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. Use the **no** command to revert to default setting.

Example

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

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

6-3 clear arp-cache (Hybrid Mode Only)

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#
```

6-4 ip address

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

ip address *IP-ADDRESS SUBNET-MASK*

no ip address *IP-ADDRESS SUBNET-MASK*

Parameters

IP-ADDRESS	Specifies the IP address.
SUBNET-MASK	Specifies the subnet mask for the associated IP address.

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

Example

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

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

6-5 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)#
```

6-6 show arp (Hybrid Mode Only)

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#
```

6-7 show arp timeout (Hybrid Mode Only)

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#
```

6-8 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. The interfaces can only be mgmt or VLAN 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. In the hybrid mode, only one VLAN IP interface is supported.

Example

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

```
Switch#show ip interface brief


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

Total Entries: 2

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
  IP Directed Broadcast is disabled
  gratuitous-send is disabled, interval is 0 seconds

Total Entries: 1

Switch#
```

7. Basic IPv6 Commands (Hybrid Mode Only)

7-1 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#
```

7-2 ipv6 address

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

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

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

Parameters

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

Default

None.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The IPv6 address can directly be specified by the user.

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
```

7-3 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

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

Example

This example shows how to add an IPv6 address incidence.

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

7-4 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 keyword causes a default route to be installed using that default router. The default keyword can be specified only on one interface.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

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

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

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)#
```

7-5 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)#
```

7-6 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** *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 vlan 1 00-01-80-11-22-99
Switch(config)#
```

7-7 show ipv6 interface

This command is used to display IPv6 interface information.

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

Parameters

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

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

This example shows how to display IPv6 interface information.

```
Switch# show ipv6 interface vlan2

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

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


Total Entries: 1

Switch#
```

7-8 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.

8. Cable Diagnostics Commands (Hybrid Mode Only)

8-1 test cable-diagnostics

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

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

Parameters

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

Default

None.

Command Mode

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#
```

8-2 show cable-diagnostics

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

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

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface's ID. The acceptable interface will be a physical port.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

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#
```

8-3 clear cable-diagnostics

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

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

Parameters

all	Specifies to clear cable diagnostics results for all interfaces.
interface *INTERFACE-ID*	Specifies the interface's ID. The acceptable interface will be a physical port.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

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#
```

9. Command Logging Commands

9-1 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)#
```

10. Debug Commands

10-1 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 the debug message output option.

Example

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

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

10-2 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. Leave a space between modules.
all	Specifies to output the debug messages of all modules to the specified destination.
buffer	Specifies to output the debug message to the debug buffer.
console	Specifies to output the debug messages to the local console.

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 configure all the module's debug messages to output to the debug buffer.

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

10-3 debug reboot on-error

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

debug reboot on-error

no debug reboot on-error

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

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

10-4 debug copy

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

debug copy *SOURCE-URL DESTINATION-URL*

debug copy *SOURCE-URL* **{tftp:** *//LOCATION/DESTINATION-URL* **| ftp:** *//USER-NAME:PASSWORD@LOCATION:TCP-PORT/DESTINATION-URL* **| rcp:** *//USER-NAME@LOCATION/DESTINATION-URL***}**

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 address of the TFTP/FTP server, or the IPv4 address of the RCP server.
USER-NAME	Specifies the user name on the FTP/RCP server.
PASSWORD	Specifies the password for the user.

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.

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#
```

10-5 debug clear buffer

This command is used to clear the debug buffer.

debug clear buffer

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to clear the debug buffer information.

Example

This example shows how to clear the debug buffer information.

```
Switch# debug clear buffer
Switch#
```

10-6 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#
```

10-7 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 optional parameter is specified, this will display the content in the buffer.

Example

This example shows how to display the debug buffer information.

```
Switch# debug show buffer

Debug buffer is empty

Switch#
```

This example shows how to display the debug buffer utilization.

```
Switch# debug show buffer utilization

Debug buffer is allocated from system memory
Total size is 2M
Utilization is 30%

Switch#
```

10-8 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
-----------------     --------  ---------------------------------------
OFS                   buffer    No

Switch#
```

10-9 debug show error-log

This command is used to display error log information.

debug show error-log

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

This example shows how to display error log information.

```
Switch# debug show error-log

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

Current TASK : bcmARL.0
------------------------- TASK STACKTRACE -------------------------
->802ACE98
->8018C814
->8028FF44
```

```
->8028352C
->801D703C
->8013B8A4
->802AE754
->802A5E0C
->802A5D6C

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

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

Total Log : 2

Switch#
```

10-10 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. If not specified, all units are displayed.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#                     DGS-3630-28PC Gigabit Ethernet Switch
#                         Technical Support Information
#
#                           Firmware: Build 2.25.013
#    Copyright(C) 2021  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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

[SYS 2021-3-15 17:11:49]

Boot Time           : 15 Mar 2021  16:00:48
RTC Time            : 2021/03/15 17:11:49
Boot PROM Version   : Build 2.10.001
Firmware Version    : Build 2.25.013
Hardware Version    : A1
Serial number       : DGS3630-28PC1
MAC Address         : F0-7D-68-30-36-00
MAC Address Number  : 65535

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

10-11 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 -  15 %         One minute -  14 %         Five minutes -  14 %

Process Name         5Sec     1Min     5Min
-----------------   ------   ------   ------
tIdleTask0           85 %     86 %     86 %
bcmL2X.0              6 %      5 %      5 %
bcmCNTR.0             4 %      3 %      3 %
NICRX                 0 %      0 %      0 %
cpuprotect            0 %      0 %      0 %
MAUMIB_TASK           0 %      0 %      0 %
bcmLINK.0             0 %      0 %      0 %
socdmadesc.0          0 %      0 %      0 %
bcmRX                 0 %      0 %      0 %
8021xCtrl             0 %      0 %      0 %
bcmIbodSync.0         0 %      0 %      0 %
hisr1                 0 %      0 %      0 %
CNT_TASK              0 %      0 %      0 %
HISTORCNT_TASK        0 %      0 %      0 %
CLI                   0 %      0 %      0 %
OS_TIMER              0 %      0 %      0 %
QOS_CNT               0 %      0 %      0 %
EEE_LLDPTask          0 %      0 %      0 %
DLKtimer              0 %      0 %      0 %
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

11. Digital Diagnostics Monitoring (DDM) Commands (Hybrid Mode Only)

11-1 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#
```

11-2 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)#
```

11-3 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 25 when an alarm event is detected.

```
Switch# configure terminal
Switch(config)# interface eth1/0/25
Switch(config-if)# transceiver-monitoring action shutdown alarm
Switch(config-if)#
```

11-4 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 21.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring bias-current eth1/0/21 high warning 10.237

WARNING: A closest value 10.236 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

11-5 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 21.

```
Switch# configure terminal
Switch(config)# interface eth1/0/21
Switch(config-if)# transceiver-monitoring enable
Switch(config-if)#
```

11-6 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 21.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring rx-power eth1/0/21 low warning mwatt 0.135
Switch(config)#
```

11-7 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 21.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring temperature eth1/0/21 high alarm 127.994

WARNING: A closer value of 127.992 is chosen according to the transceiver-monitoring precision
definition

Switch(config)#
```

11-8 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 21.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring tx-power eth1/0/21 low warning mwatt 0.181
Switch(config)#
```

11-9 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 25.

```
Switch# configure terminal
Switch(config)# transceiver-monitoring voltage eth1/0/25 low alarm 0.005
Switch(config)#
```

12. External Alarm Commands (Hybrid Mode Only)

12-1 show external-alarm

This command is used to display the status of the external alarm.

show external-alarm [unit *UNIT-ID* **[- | ,]]**

Parameters

Unit *UNIT-ID*	Specifies the unit ID to be displayed.
,	(Optional) Specifies a series of unit IDs, or separate a range of unit IDs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of unit IDs. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the status of the external alarm.

Example

This example shows how to display the status of the external alarm.

```
Switch#show external-alarm

  Channel: 1
    Status: Normal
    Message: External Alarm 1

  Channel: 2
    Status: Normal
    Message: External Alarm 2

Switch#
```

12-2 external-alarm message

This command is used to enable monitoring the external alarm source status or to configure external alarm message for a channel. Use the **no** form of this command to disable monitoring the external alarm source status or to reset external alarm message for a channel.

external-alarm [unit *UNIT-ID***] [channel** *NUMBER* **message** *SENTENCE***]**

no external-alarm [unit *UNIT-ID***] [channel** *NUMBER* **message]**

Parameters

UNIT-ID	Specifies the unit ID to be configured.
channel *NUMBER*	Specifies the channel to be configured. The range is from 1 to 2.
message *SENTENCE*	Specifies the alarm message associated with the channel with a maximum of 128 characters.

Default

By default, the alarm message is “External Alarm” followed by the channel ID.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The source of alarm is located outside of the Switch and is monitored via pre-defined connecting channels. Each channel represents a specific alarm event. The status of an alarm source can be either in the alarm state or in the normal state. If the source is absent, or the source is present and in the normal state, the status will be normal. The status will be abnormal if the source is in the abnormal state. A notification will be sent when the monitoring status is changed.

Example

This example shows how to configure the alarm message.

```
Switch#configure terminal
Switch(config)#external-alarm unit 1 channel 1 message External Alarm of UPS
Switch(config)#
```

12-3 snmp-server enable traps external-alarm

This command is used to enable the sending of the SNMP traps for the external alarm. Use the **no** form of this command to disable the function

snmp-server enable traps external-alarm

no snmp-server enable traps external-alarm

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 sending of the SNMP traps for the external alarm.

Example

This example shows how to enable the sending of the SNMP traps for the external alarm.

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

13. File System Commands

13-1 cd

This command is used to change the current directory.

cd [*DIRECTORY-URL***]**

Parameters

DIRECTORY-URL	(Optional) Specifies the URL of the directory. If 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, then 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   -rw      15433724 Feb 07 2021 15:54:55  runtime.had
2   -rw      15466640 Mar 13 2021 14:51:40  firmware.had
3   -rw          3088 Apr 11 2021 15:47:01  config.cfg
4   -rw      15478860 Mar 21 2021 14:06:29  fw5.had
5   d--             0 Apr 11 2021 15:47:46  system

1064828928 bytes total (993763328 bytes free)

Switch#cd d:
Switch#
```

This example shows how to display the current directory.

```
Switch#cd
Current directory is /c:
Switch#
```

13-2 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#
```

13-3 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 23 2000 03:49:07  c:

0 bytes total (0 bytes free)

Switch#
```

13-4 format

This command is used to format the external storage device.

format *FILE-SYSTEM* **[fat32 | fat16]**

Parameters

FILE-SYSTEM	Specifies the file system.
fat32	(Optional) Specifies to format to the FAT32 file system.
fat16	(Optional) Specifies to format to the FAT16 file system.

Default

By default, the format is FAT32.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Only the external storage can be formatted. The selected storage will be formatted to FAT32 file system by default.

Example

This example shows how to format an external Secure Digital (SD) card.

```
Switch# format /d:

All sectors will be erased, proceed? (y/n) [n] y
Enter volume id (up to 11 characters):Profiles
Format completed.

Switch#
```

13-5 mkdir

This command is used to create a directory under the current directory.

mkdir *DIRECTORY-NAME*

Parameters

DIRECTORY-NAME	Specifies the name of the directory.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to make a directory in the current directory.

Example

This example shows how to create a directory named “newdir” under the current directory.

```
Switch# mkdir newdir
Switch#
```

13-6 more

This command is used to display the contents of a file.

more *FILE-URL*

Parameters

FILE-URL	Specifies the URL for the file to be displayed.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the contents of a file in the file system. The command is usually used to display text files. If the content of a file contains non-standard printable characters, the display will feature unreadable characters or even blank spaces.

Example

This example shows how to display the contents of file “config.cfg”.

```
Switch#more c:/config.cfg


!----------------------------------------------------------------------------
!                     DGS-3630-28PC Gigabit Ethernet Switch
!                                Configuration
!
!                            Firmware: Build 2.25.013
!           Copyright(C) 2021 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

crypto pki trustpoint TP1
!
# AAA START
aaa new-model
!
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
enable password level 1 0 basic
enable password level 2 0 2
enable password level 3 0 advance
enable password level 4 0 4
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

13-7 rename

This command is used to rename a file.

rename *FILE-URL1 FILE-URL2*

Parameters

FILE-URL1	Specifies the URL for the file to be renamed.
FILE-URL2	Specifies the URL after file renaming.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

A file can be renamed to a file located either within the same directory or to another directory.

Example

This example shows how to rename file called “doc.1” to “test.txt”.

```
Switch# rename /c:/doc.1 /c:/test.txt

Rename file doc.1 to text.txt? (y/n) [n] y

Switch#
```

13-8 rmdir

This command is used to remove a directory in the file system.

rmdir *DIRECTORY-NAME*

Parameters

DIRECTORY-NAME	Specifies the name of the directory.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to remove a directory in the working directory.

Example

This example shows how to remove a directory called “newdir” under the current directory.

```
Switch# rmdir newdir

Remove directory newdir? (y/n) [n] y
The directory is removed

Switch#
```

13-9 show storage media-info

This command is used to display the storage media’s information.

show storage media-info [unit *UNIT-ID***]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the unit ID.

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.

Example

This example shows how to display the information of the storage media.

```
Switch#show storage media-info

Unit  Drive  Media-Type  Size      FS-Type  Label
----  -----  ----------  --------  -------  -----------
1     c:     Flash       1015 MB   FFS

Switch#
```

Display Parameters

Media-Type	**Flash:** This represents the storage in the Switch.

	SD Card: This represents removable storage devices including the USB flash drives.

14. Filter Database (FDB) Commands (Hybrid Mode Only)

14-1 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#
```

14-2 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)#
```

14-3 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)#
```

14-4 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 separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
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)#
```

14-5 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.

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)#
```

14-6 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)#
```

14-7 show mac-address-table

This command is used to display a specific MAC address entry or the MAC address entries for a specific interface or VLAN.

show mac-address-table [dynamic | static] [address *MAC-ADDR* **| interface [***INTERFACE-ID* **| vlan** *VLAN-ID***]**

Parameters

dynamic	(Optional) Specifies to display dynamic MAC address table entries only.
static	(Optional) Specifies to display static MAC address table entries only.
address *MAC-ADDR*	(Optional) Specifies the 48-bit MAC address.
interface *INTERFACE-ID*	(Optional) Specifies 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 option **interface** is specified, the unicast entry that has the forwarding interface matches the specified interface will be displayed

Example

This example shows how to display all the MAC address table entries for the MAC address 00-23-7D-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#
```

14-8 show mac-address-table aging-time

This command is used to display the MAC address table's aging time.

show mac-address-table aging-time

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the MAC address table's aging time.

Example

This example shows how to display the MAC address table's aging time.

```
Switch# show mac-address-table aging-time

Aging Time is 300 seconds

Switch#
```

14-9 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 separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
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 optional parameter is specified, all physical ports will be displayed.

Example

This example shows how to display the MAC address learning status on all physical ports 1 to 10.

```
Switch#show mac-address-table learning interface 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#
```

14-10 show mac-address-table notification change

This command is used to display the MAC address notification configuration or history content.

show mac-address-table notification change [interface [*INTERFACE-ID*] | history]

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the 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 option is specified, the global configuration will be displayed. Use the **interface** keyword to display information about all interfaces. If the interface ID is included, the specified interface will be displayed.

Example

This example shows how to display the MAC address notification change configuration on all interfaces.

```
Switch#show mac-address-table notification change interface

Interface                Added Trap       Removed Trap
-----------------------  --------------   --------------

eth1/0/1                 Disabled         Disabled
eth1/0/2                 Disabled         Disabled
eth1/0/3                 Disabled         Disabled
eth1/0/4                 Disabled         Disabled
eth1/0/5                 Disabled         Disabled
eth1/0/6                 Disabled         Disabled
eth1/0/7                 Disabled         Disabled
eth1/0/8                 Disabled         Disabled
eth1/0/9                 Disabled         Disabled
eth1/0/10                Disabled         Disabled
eth1/0/11                Disabled         Disabled
eth1/0/12                Disabled         Disabled
eth1/0/13                Disabled         Disabled
eth1/0/14                Disabled         Disabled
eth1/0/15                Disabled         Disabled
eth1/0/16                Disabled         Disabled
eth1/0/17                Disabled         Disabled
eth1/0/18                Disabled         Disabled
eth1/0/19                Disabled         Disabled
eth1/0/20                Disabled         Disabled
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#
```

14-11 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 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)#
```

14-12 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)#
```

15. Interface Commands

15-1 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 to clear counters for the specified interfaces. The interfaces can only be physical port or port-channel interfaces. Port-channel interface is only available in the hybrid mode.
,	(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 only available for physical port interface configuration.

Use this command to clear counters for the specified interfaces.

Example

This example shows how to clear the counters on port 1.

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

15-2 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)#
```

15-3 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. **(Hybrid Mode Only)**
- **mgmt** - Specifies the Ethernet interface used for the out-of-band management port.
- **Port-channel** - Specifies the aggregated port-channel interface. **(Hybrid Mode Only)**
- **Vlan** - Specifies the VLAN interface. **(Hybrid Mode Only)**

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.

L2vlan interface mode is only used to add descriptions to existed L2 VLANs. The **interface l2vlan** parameter does not create any new interface, and the no form of this command does not removed any existing interface.

Example

This example shows how to enter the interface configuration mode through 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)#
```

15-4 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

This command enters the interface configuration mode for the specified range of interfaces. Commands configured in the interface range mode, applies to interfaces in the range.

Example

This example shows how to enter the interface configuration mode for 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)#
```

15-5 show counters

This command is used to display interface information.

show counters [interface *INTERFACE-ID***]**

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed. If no interface is specified, counters of all interfaces will be displayed. The interfaces can only be physical port or port-channel interfaces. Port-channel interface is only available in the hybrid mode.

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.

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                     : 407
txHCTotalPkts                     : 662
rxHCUnicastPkts                   : 236
txHCUnicastPkts                   : 80
rxHCMulticastPkts                 : 73
txHCMulticastPkts                 : 567
rxHCBroadcastPkts                 : 98
txHCBroadcastPkts                 : 15
rxHCOctets                        : 40310
txHCOctets                        : 99899
rxHCPkt64Octets                   : 51
rxHCPkt65to127Octets              : 301
rxHCPkt128to255Octets             : 53
rxHCPkt256to511Octets             : 2
rxHCPkt512to1023Octets            : 0
rxHCPkt1024to1518Octets           : 0
rxHCPkt1519to1522Octets           : 0
rxHCPkt1519to2047Octets           : 0
rxHCPkt2048to4095Octets           : 0
rxHCPkt4096to9216Octets           : 0
rxHCPkt9217to16383Octets          : 0
txHCPkt64Octets                   : 471
txHCPkt65to127Octets              : 49
txHCPkt128to255Octets             : 53
txHCPkt256to511Octets             : 39
txHCPkt512to1023Octets            : 37
txHCPkt1024to1518Octets           : 13
txHCPkt1519to1522Octets           : 0
txHCPkt1519to2047Octets           : 0
txHCPkt2048to4095Octets           : 0
txHCPkt4096to9216Octets           : 0
txHCPkt9217to16383Octets          : 0

rxCRCAlignErrors                  : 0
rxUndersizedPkts                  : 0
rxFragmentPkts                    : 0
rxSymbolErrors                    : 0
rxBufferFullDropPkts              : 0
rxACLDropPkts                     : 0
rxMulticastDropPkts               : 0
rxVLANIngressCheckDropPkts        : 0
rxIpv6DropPkts                    : 0
rxSTPDropPkts                     : 0
rxStormAndTableDropPkts           : 0
rxMTUDropPkts                     : 0

txCollisions                      : 0
ifInErrors                        : 0
ifOutErrors                       : 0
ifInDiscards                      : 0
ifOutDiscards                     : 0
```

```
txDelayExceededDiscards           : 0
txCRC                             : 0
txSTPDropPkts                     : 0
txHOLDropPkts                     : 0
txCoS0DropPkts                    : 0
txCoS1DropPkts                    : 0
txCoS2DropPkts                    : 0
txCoS3DropPkts                    : 0
txCoS4DropPkts                    : 0
txCoS5DropPkts                    : 0
txCoS6DropPkts                    : 0
txCoS7DropPkts                    : 0

dot3StatsSingleColFrames          : 0
dot3StatsMultiColFrames           : 0
dot3StatsDeferredTransmissions    : 0
dot3StatsLateCollisions           : 0
dot3StatsExcessiveCollisions      : 0
dot3StatsInternalMacTransmitErrors : 0
dot3StatsFrameTooLongs            : 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).
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).
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, and dot3StatsInternalReceiveError.
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.
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.
txCoS0DropPkts	Transmit COS 0 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 0.
txCoS1DropPkts	Transmit COS 1 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 1.
txCoS2DropPkts	Transmit COS 2 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 2.
txCoS3DropPkts	Transmit COS 3 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 3.
txCoS4DropPkts	Transmit COS 4 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 4.
txCoS5DropPkts	Transmit COS 5 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 5.
txCoS6DropPkts	Transmit COS 6 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 6.
txCoS7DropPkts	Transmit COS 7 Drop Packet Counter. Incremented for each packet drop due to Head of Line blocking per egress port COS 7.
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.
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.
dot3StatsFrameTooLongs	Receive Frame Too Long Counter. Incremented for each frame received which exceeds the max-rcv-frame-size.

15-6 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. Port-channel and VLAN interfaces are only available in the hybrid mode.
,	(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 interface information.

```
Switch#show interfaces

Eth1/0/1 is enabled link status is up
  Interface type: 1000BASE-T
  Interface description:
  MAC Address: F0-7D-68-30-37-00
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1536 bytes
  Log link-status state: on
  Last Linkchange  0:1:16:24
  RX rate: 488 bits/sec, TX rate: 0 bits/sec
  RX bytes: 39643, TX bytes: 0
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 442, TX packets: 0
  RX multicast: 71, RX broadcast: 371
  RX CRC error: 0, RX undersize: 0
  RX fragment: 0, RX dropped Pkts: 442
  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

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

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

```
Switch#show interfaces vlan 1

vlan1 is enabled, Link status is up
  Interface type: VLAN
  Interface description:
  MAC address: F0-7D-68-36-30-B0


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: F0-7D-68-30-37-00
  Auto-duplex, auto-speed, auto-mdix
  Send flow-control: off, receive flow-control: off
  Send flow-control oper: off, receive flow-control oper: off
  Full-duplex, 1Gb/s
  Maximum transmit unit: 1536 bytes
  Log link-status state: on
  Last Linkchange  0:1:16:24
  RX rate: 0 bits/sec, TX rate: 0 bits/sec
  RX bytes: 41519, TX bytes: 0
  RX rate: 0 packets/sec, TX rate: 0 packets/sec
  RX packets: 471, TX packets: 0
  RX multicast: 73, RX broadcast: 398
  RX CRC error: 0, RX undersize: 0
  RX fragment: 0, RX dropped Pkts: 471
  RX MTU exceeded: 0
  TX CRC error: 0, TX excessive deferral: 0
  TX single collision: 0, TX excessive collision: 0
  TX late collision: 0, TX collision: 0


Switch#
```

This example shows how to display the interface information for management port 0.

```
Switch#show interfaces mgmt 0

mgmt_ipif 0 is enabled, Link status is up
  Interface type: Management port
  Interface description:

Switch#
```

15-7 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 not specified, the general statistics counters will be displayed.
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.

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          CrcAlign-Err /         Undersize /
              Rcv-Err /              InDiscard /
              Xmit-Err               OutDiscard
------------ ---------------------- ----------------------
eth1/0/1      0                      0
              0                      10
              0                      0
eth1/0/3      0                      0
              0                      0
              0                      0

Port          Single-Col /           Excess-Col /
              Multi-Co /             Runts /
              Late-Col               Symbol-Err
------------ ---------------------- ----------------------
eth1/0/1      0                      0
              0                      0
              0                      0
eth1/0/3      0                      0
              0                      0
              0                      0

Port          DeferredTx             IntMacTx
------------ ---------------------- ----------------------
eth1/0/1      0                      0
eth1/0/3      0                      0

Total Entries:2


Switch#
```

Display Parameters

CrcAlign-Err	Refer to the item “dot3StatsAlignmentErrors” 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.
Runts	Incremented for each packet whose size is less than 64 bytes in length.
Symbol-Err	Refer to the item “rxSymbolErrors” 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.
InDiscard	Refer to the item “ifInDiscards” 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 : 28 Dec 2021  10:53:15
Endtime   : 28 Dec 2021  10:38:15
rxHCTotalPkts                    : 0
txHCTotalPkts                    : 0
rxHCUnicastPkts                  : 0
txHCUnicastPkts                  : 0
rxHCMulticastPkts                : 0
txHCMulticastPkts                : 0
rxHCBroadcastPkts                : 0
txHCBroadcastPkts                : 0
rxHCOctets                       : 0
txHCOctets                       : 0
rxHCPkt64Octets                  : 0
rxHCPkt65to127Octets             : 0
rxHCPkt128to255Octets            : 0
rxHCPkt256to511Octets            : 0
rxHCPkt512to1023Octets           : 0
rxHCPkt1024to1518Octets          : 0
rxHCPkt1519to1522Octets          : 0
rxHCPkt1519to2047Octets          : 0
rxHCPkt2048to4095Octets          : 0
rxHCPkt4096to9216Octets          : 0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

15-8 show interfaces status

This command is used to display the Switch’s port connection status.

show interfaces [*INTERFACE-ID* **[, | -]] status**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the connection status of all switch ports will be displayed.
,	(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 Switch's port connection status.

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      not-connected 1            auto    auto           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(c)  not-connected 1            auto    auto           1000BASE-T
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

15-9 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.

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 2021  14:56:13 - 9  Apr 2021  14:41:13  : 0   %
9  Apr 2021  14:41:13 - 9  Apr 2021  14:26:13  : 0   %
9  Apr 2021  14:26:13 - 9  Apr 2021  14:11:13  : 0   %
9  Apr 2021  14:11:13 - 9  Apr 2021  13:56:13  : 0   %
9  Apr 2021  13:56:13 - 9  Apr 2021  13:41:13  : 0   %

Switch#
```

15-10 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#
```

15-11 show interfaces auto-negotiation (Hybrid Mode Only)

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

 Speed auto downgrade: Disabled
 Remote Signaling: Not detected
 Configure Status: Complete
 Capability Bits: 10M_Full, 100M_Full, 1000M_Full
 Capability Advertised Bits: 10M_Full, 100M_Full, 1000M_Full
 Capability Received Bits: 10M_Half, 10M_Full, 100M_Half, 100M_Full
 RemoteFaultAdvertised: Disabled
 RemoteFaultReceived: NoError


Switch#
```

15-12 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 to be displayed. If no interface is specified, then information related to all interfaces will be displayed. Port-channel and VLAN interfaces are only available in the hybrid mode.
,	(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 displays 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
```

15-13 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

The Physical port, loopback, VLAN, tunnel, and management interfaces are valid for this configuration. This command is also configurable for port-channel member ports.

The command will cause the port to enter the disabled state. Under the disabled state, the port will not be able to receive or transmit any packets. Using the **no shutdown** command will put the port back into the enabled state. When a port is shut down, the link status will also be turned off.

Example

This example shows how to enter the shutdown command to disable the port state on port 1.

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

16. IP Utility Commands

16-1 ping

This command is used to diagnose basic network connectivity.

ping {[ip] *IP-ADDRESS* **| [ipv6]** *IPV6-ADDRESS***} [length** *LENGTH***] [count** *TIMES***] [timeout** *SECONDS***] [stoptime** *SECONDS***] [tos** *TOS***]**

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. **(Hybrid Mode Only)**
IPV6-ADDRESS	Specifies the IPv6 address of the system to discover. **(Hybrid Mode Only)**
length *LENGTH*	(Optional) Specifies the number of data bytes to be sent. The value does not include any VLAN or IEEE 802.1Q tag length. The range is from 1 to 1420.
count *TIMES*	(Optional) Specifies to stop after sending the specified number of echo request packets.
timeout *SECONDS*	(Optional) Specifies response timeout value, in seconds.
stoptime SECONDS	(Optional) Specifies to stop pining after the specified time. If the value is 0, the pinging will never stop. The range is from 0 to 99.
tos TOS	(Optional) Specifies to configure QoS on ICMP datagrams. The range is from 0 to 255.

Default

The **length** value is 56 bytes.

The **count** value is disabled. The ping will continue until the user terminates the process.

The **timeout** value is 1 second.

The **stoptime** value is 0 (never stop).

The **tos** value is 0.

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. If neither the **count** or **timeout** value is specified, the only way to stop the ping is by pressing CTRL+C or ESC.

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#
```

16-2 traceroute (Hybrid Mode Only)

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***} [probe** *NUMBER***] [timeout** *SECONDS***] [max-ttl** *TTL***] [port** *DEST-PORT***] [length** *LENGTH***] [tos** *TOS***] [initial-ttl** *TTL***]**

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.
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.

length *LENGTH*	(Optional) Specifies the number of bytes of the outgoing datagrams. The range is from 1 to 1420.
tos TOS	(Optional) Specifies to configure ToS in the IP header of the outgoing datagrams. The range is from 0 to 255.
initial-ttl *TTL*	(Optional) Specifies to send UDP datagrams with the specified value. The allowed range is from 1 to 255.

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.

The **length** value is 12.

The **tos** value is 0.

The initial TTL is 1.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

To interrupt this command after the command has been issued, press Ctrl-C.

This command uses the TTL field in the IP header to cause routers and servers to generate specific return messages. A **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#
```

17. Jumbo Frame Commands

17-1 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 available for physical ports configuration. Oversize frames will be dropped and checks are carried out on ingress ports. Use this command to transfer large frames or jumbo frames through the Switch 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)#
```

18. Link Aggregation Control Protocol (LACP) Commands (Hybrid Mode Only)

NOTE: The Link Aggregation feature cannot be enabled on OpenFlow enabled ports.

18-1 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

The command is available for physical port interface configuration. The system will automatically create the port-channel when a physical port first joins a channel group. An interface can only join one channel-group.

If the mode **on** is specified in the command, the channel group type is static. If the mode **active** or **passive** is specified in the command, the channel group type is LACP. A channel group can only consist of either static members or LACP members. Once the type of channel group has been determined, other types of interfaces cannot join the channel group.

If the security function is enabled on a port, then this port cannot be specified as a channel group member.

Example

This example shows how to assign Ethernet interfaces 1/0/4 to 1/0/5 to a new LACP channel-group, with an ID of 3, and sets the LACP mode to active.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-5
Switch(config-if)# channel-group 3 mode active
Switch(config-if)#
```

18-2 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 interfaces 1/0/4 to 1/0/5.

```
Switch# configure terminal
Switch(config)# interface range eth1/0/4-5
Switch(config-if)# lacp port-priority 20000
Switch(config-if)#
```

18-3 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)#
```

18-4 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)#
```

18-5 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 Layer 4 destination TCP/UDP port.
src-dst-l4-port	Specifies that the Switch should examine the Layer 4 source TCP/UDP port and Layer 4 destination port
src-l4-port	Specifies that the Switch should examine the Layer 4 source TCP/UDP port.

Default

The default load-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.

- **MPLS non-terminated packets:** Use the selected field (source, destination, or source and destination) of IP address and MPLS label field to load balance the packets.
- **Layer 2 MPLS terminated packets:** Use the selected field of MAC address to load balance the packets.
- **Layer 3 MPLS terminated packets:** Use the selected field of IP address.
- **Layer 2 non-MPLS packets:** Use the selected field of MAC address when the IP address or MAC address is used as the hash key.
- **Non-MPLS IP packets:** Use the selected field of IP address when the IP address is used as the hash key. Use the selected field of MAC address when the MAC address is used as the hash key.

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)#
```

18-6 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.
  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 enhanced MPLS label

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#
```

19. Loopback Test Commands (Hybrid Mode Only)

19-1 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)#
```

19-2 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#
```

20. Network Protocol Port Protection Commands (Hybrid Mode Only)

20-1 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)#
```

20-2 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#
```

21. OpenFlow Commands

21-1 openflow global enable

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

openflow global enable

no openflow global enable

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This configuration only takes effect after it was saved and the Switch was rebooted. The OpenFlow function has two modes: **pure** and **hybrid**. By default, the hybrid mode is used. Thus, the OpenFlow function must be enabled on the specified ports by the **openflow enable** command after the OpenFlow function is globally enabled.

When OpenFlow is globally disabled on the Switch, all legacy functions will be available.

Back up the configuration before changing the OpenFlow state.

For more information, refer to the *DGS-3630 Series CLI Reference Guide*.

Example

This example shows how to disable the OpenFlow function.

```
Switch#configure terminal
Switch(config)#no openflow global enable

 WARNING: The command does not take effect until the next reboot.


Switch(config)#exit
Switch#copy running-config startup-config

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

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

Switch#reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

21-2 openflow enable

This command is used to enable the OpenFlow function on specified ports. Use the **no** form of this command to disable the OpenFlow function on specified ports.

openflow enable

no openflow enable

Parameters

None.

Default

By default, this function is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This configuration only takes effect after it was saved and the Switch was rebooted. Use this command to enable or disable the OpenFlow function on specified ports.

This configuration only takes effect when the OpenFlow function is globally enabled and is configured to use the hybrid mode.

NOTE: Link Aggregation and STP cannot be enabled on OpenFlow enabled ports.

Example

This example shows how to enable the OpenFlow function on port 2 to 5.

```
Switch#configure terminal
Switch(config)#openflow global enable

 WARNING: The command does not take effect until the next reboot.


Switch(config)#interface range eth1/0/2-5
Switch(config-if-range)#openflow enable

 WARNING: The command does not take effect until the next reboot.


Switch(config-if-range)#end
Switch#copy running-config startup-config

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

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

Switch#reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

21-3 openflow controller

This command is used to configure the OpenFlow controller. Use the **no** form of this command to remove an OpenFlow controller.

openflow controller *IP-ADDRESS* **[service-port** *TCP-PORT***] [connection {tcp | tls}]**

no openflow controller *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IP address of the OpenFlow controller.
service-port *TCP-PORT*	(Optional) Specifies the TCP port number used for the connection between the Switch and the OpenFlow controller. The range is from 1 to 65535.
connection	(Optional) Specifies the connection type between the Switch and the OpenFlow controller. • tcp - Specifies to use the TCP connection. • tls - Specifies to use the TLS connection.

Default

By default, the port number is 6653.

By default, the connection type is TCP.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

An OpenFlow control packet, sent from the management port, will always be untagged. The maximum number of controllers is 4.

Example

This example shows how to add an OpenFlow controller with the IP address of 192.168.1.1 and the port number of 6666 using the TLS connection.

```
Switch#configure terminal
Switch(config)# openflow controller 192.168.1.1 service-port 6666 connection tls
Switch(config)#
```

21-4 openflow mode

This command is used to configure the OpenFlow mode. Use the **no** form of this command to revert to the default setting.

openflow mode {pure | hybrid}

no openflow mode

Parameters

pure	Specifies to use the pure mode.
hybrid	Specifies to use the hybrid mode.

Default

By default, the hybrid mode is used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This configuration only takes effect after it was saved and the Switch was rebooted.

Use this command to specify the OpenFlow mode as **pure** or **hybrid**.

In the **pure** mode, all the ports on the Switch will be used in the OpenFlow pipeline. The OpenFlow controller can only be connected to the management port.

In the **hybrid** mode, a port can be configured to use the OpenFlow pipeline or not. Use the **openflow enable** command in the Interface Configuration Mode to specify whether a port uses the OpenFlow pipeline or not. The OpenFlow controller can be connected to the management port and any normal port.

To ensure the OpenFlow function works properly in the hybrid mode, some legacy settings need to be modified:

- Configure the **flowcontrol** command to **off**.
- Configure the **port-channel load-balance** command to use the Layer 4 TCP/UDP port algorithm.

Example

This example shows how to specify to use the pure mode.

```
Switch#configure terminal
Switch(config)#openflow mode pure

 WARNING: The command does not take effect until the next reboot.


Switch(config)#end
Switch#copy running-config startup-config

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

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

Switch#reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

This example shows how to specify to use the hybrid mode.

```
Switch#configure terminal
Switch(config)#openflow global enable

 WARNING: The command does not take effect until the next reboot.


Switch(config)#openflow mode hybrid
Switch(config)#interface range eth1/0/2-5
Switch(config-if-range)#openflow enable

 WARNING: The command does not take effect until the next reboot.


Switch(config-if-range)#flowcontrol off
Switch(config-if-range)#exit
Switch(config)#port-channel load-balance src-l4-port
Switch(config)#end
Switch#copy running-config startup-config

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

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

Switch#reboot

Are you sure you want to proceed with the system reboot?(y/n) y
Please wait, the switch is rebooting...
```

21-5 openflow fail-mode

This command is used to configure the connection-fail mode. Use the **no** form of this command to revert to the default setting.

openflow fail-mode {secure | standalone}

no openflow fail-mode

Parameters

secure	Specifies to use the fail secure mode.
standalone	Specifies to use the fail standalone mode.

Default

By default, **secure** is used.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the OpenFlow connection-fail mode as **secure** or **standalone**. When the Switch loses contact with all controllers, the Switch will enter the OpenFlow connection-fail mode.

- **Fail secure mode:** The Switch stops sending packets to the controller. Flow entries continue to expire based on their timeouts.
- **Fail standalone mode:** This is only available in the hybrid mode. The Switch stops sending packets to the controller. Flow entries are removed from the OpenFlow-enabled ports. Legacy functions on legacy ports are not affected.

Example

This example shows how to specify to use the fail standalone mode.

```
Switch#configure terminal
Switch(config)#openflow fail-mode standalone
Switch(config)#
```

21-6 openflow table-miss

This command is used to configure the table-miss entry. Use the **no** form of this command to remove the table-miss entry.

openflow table-miss action {drop | to-controller}

no openflow table-miss

Parameters

drop	Specifies to initiate the Clear-Actions instruction for the table-miss entry. This instruction specifies that unknown packets will be dropped.
to-controller	Specifies to initiate the Apply-Actions instruction for the table-miss entry. This instruction specifies that unknown packets will be sent to a controller.

Default

By default, no table-miss entry is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The table-miss flow entry specifies how unmatched packets are processed by other flow entries in the flow table. A table-miss flow entry is identified by its match and priority. It wildcards all match fields (all fields omitted) and has the lowest priority (0).

Example

This example shows how to configure a table-miss entry to send unknown packets to the controller.

```
Switch#configure terminal
Switch(config)# openflow table-miss action to-controller
Switch(config)#
```

21-7 clear openflow statistics

This command is used to clear the statistics information from the flow table.

clear openflow statistics [cookie *COOKIE-ID***]**

Parameters

cookie *COOKIE-ID*	(Optional) Specifies the cookie ID of the flow entry. This ID can be up to 16 hexadecimal digits long.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

All statistics information will be cleared if the cookie ID is not specified.

Example

This example shows how to clear the statistics information from the flow entry with the cookie ID of 0x000100001E5EA766.

```
Switch# clear openflow statistics cookie 0x000100001E5EA766
Switch#
```

21-8 show openflow configuration

This command is used to display the OpenFlow configuration.

show openflow configuration

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the OpenFlow configuration.

Example

This example shows how to display the OpenFlow configuration.

```
Switch#show openflow configuration

OpenFlow Admin State : Enabled
OpenFlow Opera State : Enabled
OpenFlow Admin Mode  : Hybrid
OpenFlow Opera Mode  : Hybrid
OpenFlow Admin Ports : 1/0/2-1/0/28
OpenFlow Opera Ports : 1/0/2-1/0/28
Connection Fail Mode : Secure

OpenFlow Controller    :
IP address      Port  Connection Role    Status
--------------- ----- ---------- ------- ------
20.20.20.2      6653  TCP        Equal   Down
192.200.200.253 65535 TLS        Equal   Down
223.254.254.253 65535 TCP        Equal   Down
223.254.254.254 1     TLS        Equal   Down

Total Entries: 4
```

21-9 show openflow table

This command is used to display OpenFlow table information.

show openflow table [detail]

Parameters

detail	(Optional) Specifies to display detailed OpenFlow table information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Brief OpenFlow table information will be displayed if the **detail** parameter is not specified.

Example

This example shows how to display brief OpenFlow table information.

```
Switch#show openflow table

<table 0>
    active_entry = 0
    lookup_count = (N/A)
    match_count  = (N/A)
    max_entries  = 1920
    INSTRUCTIONS :
        write_actions : group
        apply_actions : output, set_field
        clear_actions : (Support)
        goto_table    : -
        metadata = (Not Support)     , metadata_mask = (Not Support)
    MATCH :
        in_port in_phy_port eth_dst eth_src eth_type vlan_vid vlan_pcp ip_dscp ip_proto
ipv4_src ipv4_dst tcp_src tcp_dst udp_src udp_dst sctp_src sctp_dst arp_spa ipv6_src ipv6_dst
    Table-Miss Entry Admin State: -

Switch#
```

This example shows how to display detailed OpenFlow table information.

```
Switch#show openflow table detail

<table 0>
    active_entry = 0
    lookup_count = (N/A)
    match_count  = (N/A)
    max_entries  = 1920
    metadata match = (Not Support)
    metadata write = (Not Support)
    INSTRUCTIONS :
        write_actions : group
        apply_actions : output, set_field
        clear_actions : (Support)
        goto_table    : -
        metadata = (Not Support)     , metadata_mask = (Not Support)
    MATCH :
        in_port in_phy_port eth_dst eth_src eth_type vlan_vid vlan_pcp ip_dscp ip_proto
ipv4_src ipv4_dst tcp_src tcp_dst udp_src udp_dst sctp_src sctp_dst arp_spa ipv6_src ipv6_dst
    WRITE_ACTIONS :
        group
    APPLY_ACTIONS :
        output, set_field
    WRITE_SETFIELD :
        (Not Support)
    APPLY_SETFIELD :
        vlan_pcp ip_dscp ip_ecn
    Table-Miss Entry Admin State: -

Switch#
```

Display Parameters

active_entry	The number of active entries.
lookup_count	The number of packets looked up in the table.
matched_count	The number of packets that hit the table.
metadata match	Bits of metadata that the table can match.
metadata write	Bits of metadata that the table can write.
INSTRUCTIONS	Each flow entry contains a set of instructions that are executed when a packet matches the entry.
write_actions	The action list that write_actions support.
apply_actions	The action list that apply_actions support.
clear_actions	The action list that clear_actions support. It only supports Drop.
goto_table	There is only one flow table. It does not support the goto_table.
metadata	A maskable register value that is used to carry information from one table to the next.
MATCH	The supported list of match fields.
WRITE_ACTIONS	The list of actions that write_actions support.
APPLY_ACTIONS	The list of actions that apply_actions support.
WRITE_SETFIELD	The list of set_fields that is supported in the WRITE_ACTIONS.
APPLY_SETFIELD	The list of set_fields that is supported in the APPLY_ACTIONS.

21-10 show openflow flows

This command is used to display information related to OpenFlow flows.

show openflow flows

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display information related to OpenFlow flows.

Example

This example shows how to display information related to OpenFlow flows.

```
Switch#  show openflow  flows

===
Match Fields:
 ETH_TYPE=0x0800
Priority=5
Cookie=0x000100001E5EA766
Idle timeout=0, Hard timeout=0
Table=0, Packets=0, Bytes=0
Create time=2021-04-19 13:15:25
Instructions:
 Apply-Actions: Output=CONTROLLER(Reserved)
 Clear-Actions

===
Match Fields:
 ETH_TYPE=0x0806
Priority=5
Cookie=0x0001000000747515
Idle timeout=0, Hard timeout=0
Table=0, Packets=0, Bytes=0
Create time=2021-04-19 13:15:25
Instructions:
 Apply-Actions: Output=CONTROLLER(Reserved)
 Clear-Actions

===
Match Fields:
 ETH_TYPE=0x0806
Priority=40000
Cookie=0x00010000368E49C1
Idle timeout=0, Hard timeout=0
Table=0, Packets=0, Bytes=0
Create time=2021-04-19 13:15:25
Instructions:
 Apply-Actions: Output=CONTROLLER(Reserved)
 Clear-Actions

===
Match Fields:
 ETH_TYPE=0x88CC
Priority=40000
Cookie=0x00010000988BF5B9
Idle timeout=0, Hard timeout=0
Table=0, Packets=0, Bytes=0
Create time=2021-04-19 13:15:25
Instructions:
 Apply-Actions: Output=CONTROLLER(Reserved)
 Clear-Actions

===
Match Fields:
 ETH_TYPE=0x8942
Priority=40000
```

```
Cookie=0x0001000033DD4DC9
Idle timeout=0, Hard timeout=0
Table=0, Packets=0, Bytes=0
Create time=2021-04-19 13:15:25
Instructions:
 Apply-Actions: Output=CONTROLLER(Reserved)
 Clear-Actions

Total:5

Switch#
```

21-11 show openflow group-desc

This command is used to display the content of OpenFlow group entries.

show openflow group-desc

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the content of OpenFlow group entries.

Example

This example shows how to display the content of OpenFlow group entries.

```
Switch#show show openflow group-desc

===
GroupId=65537, Hex=0x00010001 (L2 Interface, ChainId=1, Port=1)
Type=Indirect, Reference count=3
Create time=2021-04-19 13:48:13
Bucket=1: Output=1

===
GroupId=65538, Hex=0x00010002 (L2 Interface, ChainId=1, Port=2)
Type=Indirect, Reference count=2
Create time=2021-04-19 13:48:13
Bucket=1: Output=2

===
GroupId=65539, Hex=0x00010003 (L2 Interface, ChainId=1, Port=3)
Type=Indirect, Reference count=2
Create time=2021-04-19 13:48:13
Bucket=1: Output=3

===
GroupId=268435457, Hex=0x10000001 (L2 Rewrite, Id=1)
Type=Indirect, Reference count=0
Create time=2021-04-19 13:48:13
Bucket=1: Group=65537, SrcMac=00-AA-BB-CC-DD-EE, DstMac=00-01-02-03-04-05, VlanI
d=(1|present)

===
GroupId=536870913, Hex=0x20000001 (L3 Unicast, Id=1)
Type=Indirect, Reference count=1
Create time=2021-04-19 13:48:13
Bucket=1: Group=65537, Dec TTL, SrcMac=00-AA-BB-CC-DD-EE, DstMac=00-01-02-03-04-05,
VlanId=(1|present)

Total:5

Switch#
```

21-12 show openflow meter-config

This command is used to display the content of OpenFlow meter entries.

show openflow meter-config

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the content of OpenFlow meter entries.

Example

This example shows how to display the content of OpenFlow meter entries.

```
Switch# show openflow meter-config

===
Id=1
Flags=kbps, burst
Reference count=0
Create time=2021-04-19 13:52:35
Band=1, Type=drop, Rate=10000, Burst=128

===
Id=20
Flags=pps, burst
Reference count=0
Create time=2021-04-19 13:52:54
Band=1, Type=drop, Rate=1280, Burst=640

Total:2

Switch#
```

21-13 show openflow status

This command is used to display the status of the OpenFlow function.

show openflow status [features | port-description [interface *INTERFACE-ID* **[, | -]]]**

Parameters

features	(Optional) Specifies to display the supporting status of OpenFlow features.
port-description	(Optional) Specifies to display the port descriptions of OpenFlow.
interface *INTERFACE-ID*	(Optional) Specifies the interface(s) to be displayed.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

All OpenFlow status information will be displayed if no parameter is specified.

Example

This example shows how to display the status of the OpenFlow function.

```
Switch#show openflow status

Features:
  OpenFlow Version  : v1.3
  Datapath ID       : 0000F07D68303600
  Number of buffers : No buffer
  Number of tables  : 1
  Auxiliary ID      : 0
  Flags             : Normal

  Capabilities            Status
  ----------------------- -------------
  Flow statistics         Supported
  Table statistics        Supported
  Port statistics         Supported
  Group statistics        Supported
  Reassemble IP fragments Not supported
  Queue statistics        Supported
  Port blocked            Not supported

Port Description:
  Port  Name           HW address        Config       State   Speed
  ----- -------------- ----------------- ------------ ------- --------
  1     eth1/0/1       F0-7D-68-30-37-00 -            Up      1GB_FD
  2     eth1/0/2       F0-7D-68-30-37-01 -            Down    OTHER
  3     eth1/0/3       F0-7D-68-30-37-02 -            Down    OTHER
  4     eth1/0/4       F0-7D-68-30-37-03 -            Down    OTHER
  5     eth1/0/5       F0-7D-68-30-37-04 -            Down    OTHER
  6     eth1/0/6       F0-7D-68-30-37-05 -            Down    OTHER
  7     eth1/0/7       F0-7D-68-30-37-06 -            Down    OTHER
  8     eth1/0/8       F0-7D-68-30-37-07 -            Down    OTHER
  9     eth1/0/9       F0-7D-68-30-37-08 -            Down    OTHER
  10    eth1/0/10      F0-7D-68-30-37-09 -            Down    OTHER
  11    eth1/0/11      F0-7D-68-30-37-0A -            Down    OTHER
  12    eth1/0/12      F0-7D-68-30-37-0B -            Down    OTHER
  13    eth1/0/13      F0-7D-68-30-37-0C -            Down    OTHER
  14    eth1/0/14      F0-7D-68-30-37-0D -            Down    OTHER
  15    eth1/0/15      F0-7D-68-30-37-0E -            Down    OTHER
  16    eth1/0/16      F0-7D-68-30-37-0F -            Down    OTHER
  17    eth1/0/17      F0-7D-68-30-37-10 -            Down    OTHER
  18    eth1/0/18      F0-7D-68-30-37-11 -            Down    OTHER
  19    eth1/0/19      F0-7D-68-30-37-12 -            Down    OTHER
  20    eth1/0/20      F0-7D-68-30-37-13 -            Down    OTHER
  21    eth1/0/21      F0-7D-68-30-37-14 -            Down    1GB_FD
  22    eth1/0/22      F0-7D-68-30-37-15 -            Down    1GB_FD
  23    eth1/0/23      F0-7D-68-30-37-16 -            Down    1GB_FD
  24    eth1/0/24      F0-7D-68-30-37-17 -            Down    1GB_FD
  25    eth1/0/25      F0-7D-68-30-37-18 -            Down    10GB_FD
  26    eth1/0/26      F0-7D-68-30-37-19 -            Down    10GB_FD
  27    eth1/0/27      F0-7D-68-30-37-1A -            Down    10GB_FD
  28    eth1/0/28      F0-7D-68-30-37-1B -            Down    10GB_FD

Switch#
```

21-14 debug openflow

This command is used to configure the OpenFlow debug function. Use the **no** form of this command to disable the OpenFlow debug function.

debug openflow [connection | event]

no debug openflow [connection | event]

Parameters

connection	(Optional) Specifies to display the connection type debug log.
event	(Optional) Specifies to display the event type debug log.

Default

By default, the OpenFlow debug function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

The connection type display contains debug messages for communication between the Switch and OpenFlow controllers. The event type display contains debug messages related to the state machine of the OpenFlow function.

Example

This example shows how to enable the OpenFlow debug function state and configure the debug type.

```
Switch# debug openflow
Switch# debug openflow connection
Switch# debug openflow event
Switch#
```

21-15 debug openflow flow-add

This command is used to simulate the OpenFlow OFPFC_ADD message to add flow entry.

debug openflow flow-add table 0 priority *NUM* **idle-timeout** *SECOND* **hard-timeout** *SECOND* **match {[in-port** *NUM*] **[in-phy-port** *PORT*] **[eth-src** *MACADDR MACMASK*] **[eth-dst** *MACADDR MACMASK*] **[eth-type** *HEX*] **[vlan-vid** *VLAN-ID* **present] [vlan-pcp** *INT*] **[ip-dscp** *INT*] **[ip-protocol** *INT*] **[{[ipv4-src** *IPADDR NETMASK*] **[ipv4-dst** *IPADDR NETMASK*] **| [ipv6-src** *IPV6-ADDR IPV6-ADDR*] **[ipv6-dst** *IPV6-ADDR IPV6-ADDR*] **| [arp-spa** *IPADDR NETMASK*]}] **[{[tcp-src** *INT*] **[tcp-dst** *INT*] **| [udp-src** *INT*] **[udp-dst** *INT*] **| [sctp-src** *INT*] **[sctp-dst** *INT*]}] **| none} instruction {clear-actions | {write-actions group** *NUM* **[meter** *NUM*] **|**

apply-actions [output *NUM***] [set-field vlan-pcap** *INT***] [set-field ip-dscp** *INT***] [set-field ip-ecn** *INT***] [meter** *NUM***]}}**

Parameters

priority *NUM*	Specifies the priority level of the flow entry. The range is from 0 to 65535.
idle-timeout *SECOND*	Specifies the idle timeout value befpre discarding. The valid is from 0 to 65535 seconds.
hard-timeout *SECOND*	Specifies the maximum time before discarding. The range is from 0 to 65535 seconds.
match	Specifies fields to match.
in-port *NUM*	(Optional) Specifies the input port. The range is from 1 to 4294967295.
in-phy-port *PORT*	(Optional) Specifies the physical input port on the Switch.
eth-src *MACADDR MACMASK*	(Optional) Specifies the Ethernet source MAC address with mask.
eth-dst *MACADDR MACMASK*	(Optional) Specifies the Ethernet destination MAC address with mask.
eth-type *HEX*	(Optional) Specifies the Ethernet frame type. The range is from 0x0600 to 0xFFFF.
vlan-vid *VLAN-ID* **present**	(Optional) Specifies the VLAN ID. The **present** parameter indicates packets with VLAN tag.
vlan-pcp *INT*	(Optional) Specifies the VLAN priority. The range is from 0 to 7.
ip-dscp *INT*	(Optional) Specifies the IP DSCP. The range is from 0 to 63.
ip-protocol *INT*	(Optional) Specifies the IP protocol. The range is from 0 to 255.
ipv4-src *IPADDR NETMASK*	(Optional) Specifies the source IPv4 address with mask.
ipv4-dst *IPADDR NETMASK*	(Optional) Specifies the destination IPv4 address with mask.
ipv6-src *IPV6-ADDR IPV6-ADDR*	(Optional) Specifies the source IPv6 address with mask.
ipv6-dst *IPV6-ADDR IPV6-ADDR*	(Optional) Specifies the destination IPv6 address with mask.
arp-spa *IPADDR NETMASK*	(Optional) Specifies the ARP source IPv4 address with mask.
tcp-src *INT*	(Optional) Specifies the TCP source port. The range is from 0 to 65535.
tcp-dst *INT*	(Optional) Specifies the TCP destination port. The range is from 0 to 65535.
udp-src *INT*	(Optional) Specifies the UDP source port. The range is from 0 to 65535.
udp-dst *INT*	(Optional) Specifies the UDP destination port. The range is from 0 to 65535.
sctp-src *INT*	(Optional) Specifies the SCTP source port. The range is from 0 to 65535.
sctp-dst *INT*	(Optional) Specifies the SCTP destination port. The range is from 0 to 65535.
none	Specifies to omit all fields. It wildcards all matched fields.
instruction	Specifies to modify the action set or pipeline process.
clear-actions	Specifies to clear all actions in the action set immediately.
write-actions	Specifies to merge the specified action into the current action set.
group *NUM*	Specifies the group action. The range is from 1 to 4294967040.
meter *NUM*	Specifies the meter value used by the direct packet. The range is from 1 to 4294901760.

apply-actions	Specifies that the action(s) is applied immediately without any change to the action set.
output *NUM*	Specifies the output action value. This action specifies how the packet is forwarded from the port. The range is from 1 to 4294967295.
set-field vlan-pcap *INT*	Specifies to use the Set-Files action to modify the VLAN priority. The range is from 0 to 7.
set-field ip-dscp *INT*	Specifies use the Set-Files action to modify the IP DSCP. The range is from 0 to 63.
set-field ip-ecn *INT*	Specifies use the Set-Files action to modify the IP ECN. The range is from 0 to 3.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPFC_ADD message to add flow entry.

Example

This example shows how to send 2000::15 to controller.

```
Switch# debug openflow flow-add table 0 priority 128 idle-timeout 300 hard-timeout 500 match eth-type 0x86dd ipv6-src 2000::15 FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF instruction apply-actions output 4294967293
Switch#
```

21-16 debug openflow flow-del table all

This command is used to simulate the OpenFlow OFPFC_DELETE message to delete all flow entries.

debug openflow flow-del table all

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPFC_DELETE message to delete all flow entries.

Example

This example shows how to remove all flow entries.

```
Switch# debug openflow flow-del table all
Switch#
```

21-17 debug openflow flow-del-strict

This command is used to simulate the OpenFlow OFPFC_DELETE_STRICT message to delete a flow entry.

debug openflow flow-del-strict table 0 priority *NUM* **match {[in-port** *NUM***] [in-phy-port** *PORT***] [eth-src** *MACADDR MACMASK***] [eth-dst** *MACADDR MACMASK***] [eth-type** *HEX***] [vlan-vid** *VLAN-ID* **present] [vlan-pcp** *INT***] [ip-dscp** *INT***] [ip-protocol** *INT***] [{[ipv4-src** *IPADDR NETMASK***] [ipv4-dst** *IPADDR NETMASK***] | [ipv6-src** *IPV6-ADDR IPV6-ADDR***] [ipv6-dst** *IPV6-ADDR IPV6-ADDR***] | [arp-spa** *IPADDR NETMASK***]}] [{[tcp-src** *INT***] [tcp-dst** *INT***] | [udp-src** *INT***] [udp-dst** *INT***] | [sctp-src** *INT***] [sctp-dst** *INT***]}] | none}**

Parameters

priority *NUM*	Specifies the priority level of the flow entry. The range is from 0 to 65535.
match	Specifies fields to match.
in-port *NUM*	(Optional) Specifies the input port. The range is from 1 to 4294967295.
in-phy-port *PORT*	(Optional) Specifies the physical input port on the Switch.
eth-src *MACADDR MACMASK*	(Optional) Specifies the Ethernet source MAC address with mask.
eth-dst *MACADDR MACMASK*	(Optional) Specifies the Ethernet destination MAC address with mask.
eth-type *HEX*	(Optional) Specifies the Ethernet frame type. The range is from 0x0600 to 0xFFFF.
vlan-vid *VLAN-ID* **present**	(Optional) Specifies the VLAN ID. The **present** parameter indicates packets with VLAN tag.
vlan-pcp *INT*	(Optional) Specifies the VLAN priority. The range is from 0 to 7.
ip-dscp *INT*	(Optional) Specifies the IP DSCP. The range is from 0 to 63.
ip-protocol *INT*	(Optional) Specifies the IP protocol. The range is from 0 to 255.
ipv4-src *IPADDR NETMASK*	(Optional) Specifies the source IPv4 address with mask.
ipv4-dst *IPADDR NETMASK*	(Optional) Specifies the destination IPv4 address with mask.
ipv6-src *IPV6-ADDR IPV6-ADDR*	(Optional) Specifies the source IPv6 address with mask.
ipv6-dst *IPV6-ADDR IPV6-ADDR*	(Optional) Specifies the destination IPv6 address with mask.
arp-spa *IPADDR NETMASK*	(Optional) Specifies the ARP source IPv4 address with mask.
tcp-src *INT*	(Optional) Specifies the TCP source port. The range is from 0 to 65535.
tcp-dst *INT*	(Optional) Specifies the TCP destination port. The range is from 0 to 65535.
udp-src *INT*	(Optional) Specifies the UDP source port. The range is from 0 to 65535.

udp-dst *INT*	(Optional) Specifies the UDP destination port. The range is from 0 to 65535.
sctp-src *INT*	(Optional) Specifies the SCTP source port. The range is from 0 to 65535.
sctp-dst *INT*	(Optional) Specifies the SCTP destination port. The range is from 0 to 65535.
none	Specifies to omit all fields. It wildcards all matched fields.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPFC_DELETE_STRICT message to delete a flow entry.

Example

This example shows how to remove a flow entry.

```
Switch# debug openflow flow-del-strict table 0 priority 200 match in-port 1
Switch#
```

21-18 debug openflow group-add l2-interface-group

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 2 interface group entry.

debug openflow group-add l2-interface-group *NUM* **actions output** *PORT*

Parameters

NUM	Specifies the group ID. The range is from 1 to 4294967040.
actions	Specifies the action set of the group action bucket.
output *PORT*	Specifies that the output action forwards packets to the specified OpenFlow port.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 2 interface group entry.

For more information about the group ID naming rule, refer to **Appendix D - OpenFlow Object Details**.

Example

This example shows how to create the Layer 2 interface group entry.

```
Switch# debug openflow group-add l2-interface-group 65537 actions output 1/0/1
Switch#
```

21-19 debug openflow group-add l2-rewrite-group

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 2 re-write group entry.

debug openflow group-add l2-rewrite-group *NUM* **actions group** *NUM* **[set-field eth-dst** *MACADDR***] [set-field eth-src** *MACADDR***] [set-field vlan** *VLAN-ID* **present]**

Parameters

NUM	Specifies the group ID. The range is from 1 to 4294967040.
actions	Specifies the action set of the group action bucket.
group *NUM*	Specifies the group ID that will be chained to the Layer 2 interface group. The range is from 1 to 4294967040.
set-field eth-dst *MACADDR*	(Optional) Specifies to use the Set-Files action to re-write the destination MAC address.
set-field eth-src *MACADDR*	(Optional) Specifies to use the Set-Files action to re-write the source MAC address.
set-field vlan-vid *VLAN-ID* **present**	(Optional) Specifies to use the Set-Files action to re-write the VLAN ID. The VLAN ID must be the same as the Chain ID in the chained Layer 2 interface group. The **present** parameter indicates packets with VLAN tag.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 2 re-write group entry.

For more information about the group ID naming rule, refer to **Appendix D - OpenFlow Object Details**.

Example

This example shows how to create the Layer 2 rewrite group entry.

```
Switch# debug openflow group-add l2-rewrite-group 268435457 actions group 65537 set-field eth-dst 000102030405 set-field eth-src 00aabbccddee set-field vlan 1 present
Switch#
```

21-20 debug openflow group-add l2-multicast-group

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 2 multicast group entry.

debug openflow group-add l2-multicast-group *NUM* **buckets group** *NUM* **[group** *NUM***] [group** *NUM***] [group** *NUM***]**

Parameters

NUM	Specifies the group ID. The range is from 1 to 4294967040.
buckets	Specifies the group action bucket.
group *NUM*	Specifies the group ID that will be chained to the Layer 2 interface group. The range is from 1 to 4294967040.
group *NUM*	(Optional) Specifies the group ID that will be chained to the Layer 2 interface group. The range is from 1 to 4294967040.
group *NUM*	(Optional) Specifies the group ID that will be chained to the Layer 2 interface group. The range is from 1 to 4294967040.
group *NUM*	(Optional) Specifies the group ID that will be chained to the Layer 2 interface group. The range is from 1 to 4294967040.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 2 multicast group entry.

All Layer 2 interface group entries that is refered to by the multicast group entry and the multicast group entry itself must have the same Chain ID.

For more information about the group ID naming rule, refer to **Appendix D - OpenFlow Object Details**.

Example

This example shows how to create the Layer 2 multicast group entry.

```
Switch# debug openflow group-add l2-multicast-group 805371905 buckets group 65537 group 65538 group 65539
Switch#
```

21-21 debug openflow group-add l3-unicast-group

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 3 unicast group entry.

debug openflow group-add l3-unicast-group *NUM* **actions group** *NUM* **dec-ttl set-field eth-dst** *MACADDR* **set-field eth-src** *MACADDR* **set-field vlan** *VLAN-ID* **present**

Parameters

NUM	Specifies the group ID. The range is from 1 to 4294967040.
actions	Specifies the action set of the group action bucket.
group *NUM*	Specifies the group ID that will be chained to the Layer 2 interface group. The range is from 1 to 4294967040.
dec-ttl	Specifies the decrement TTL.
set-field eth-dst *MACADDR*	(Optional) Specifies to use the Set-Files action to re-write the next hop destination MAC address.
set-field eth-src *MACADDR*	(Optional) Specifies to use the Set-Files action to re-write the source MAC address corresponding to the Layer 3 output interface.
set-field vlan-vid *VLAN-ID* **present**	(Optional) Specifies to use the Set-Files action to re-write the VLAN ID corresponding to the Layer 3 output interface. The VLAN ID must be the same as the Chain ID in the chained Layer 2 interface group. The **present** parameter indicates packets with VLAN tag.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 3 unicast group entry.

For more information about the group ID naming rule, refer to **Appendix D - OpenFlow Object Details**.

Example

This example shows how to create the Layer 3 unicast group entry.

```
Switch# debug openflow group-add l3-unicast-group 536870913 actions group 65537 dec-ttl set-field eth-dst 000102030405 set-field eth-src 00aabbccddee set-field vlan 1 present
Switch#
```

21-22 debug openflow group-add l3-ecmp-group

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 3 ECMP group entry.

debug openflow group-add l3-ecmp-group *NUM* **buckets group** *NUM* **[group** *NUM***] [group** *NUM***] [group** *NUM***]**

Parameters

NUM	Specifies the group ID. The range is from 1 to 4294967040.
buckets	Specifies the group action bucket.
group *NUM*	Specifies the group ID that will be chained to the Layer 3 unicast group. The range is from 1 to 4294967040.
group *NUM*	(Optional) Specifies the group ID that will be chained to the Layer 3 unicast group. The range is from 1 to 4294967040.
group *NUM*	(Optional) Specifies the group ID that will be chained to the Layer 3 unicast group. The range is from 1 to 4294967040.
group *NUM*	(Optional) Specifies the group ID that will be chained to the Layer 3 unicast group. The range is from 1 to 4294967040.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPGC_ADD message to add the Layer 3 ECMP group entry.

For more information about the group ID naming rule, refer to **Appendix D - OpenFlow Object Details**.

Example

This example shows how to create the Layer 3 ECMP group entry.

```
Switch# debug openflow group-add l3-ecmp-group 1879048193 buckets group 536870913 group
536870914 group 536870915
Switch#
```

21-23 debug openflow group-del

This command is used to simulate the OpenFlow OFPFC_DELETE message to delete a group entry.

debug openflow group-del {*NUM* **| all}**

Parameters

NUM	Specifies the group ID. The range is from 1 to 4294967040.
all	Specifies to delete all group entries.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPFC_DELETE message to delete a group entry.

Example

This example shows how to delete a group entry.

```
Switch# debug openflow group-del 65537
Switch#
```

21-24 debug openflow meter-add

This command is used to simulate the OpenFlow OFPGC_ADD message to add the meter entry.

debug openflow meter-add *NUM* **drop {pps | kbps} rate** *NUM* **burst** *NUM*

Parameters

NUM	Specifies the meter ID. The range is from 1 to 4294901760.
drop	Specifies to drop packets.
pps	Specifies the rate value in packet per second.
kbps	Specifies the rate value in kilo-bit per second.
rate	Specifies the rate for dropping packets. The range is from 0 to 1000000.
burst	Specifies the size of bursts. The range is from 0 to 1000000.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPGC_ADD message to add the meter entry.

Example

This example shows how to add the meter entry.

```
Switch# debug openflow meter-add 10 drop kbps rate 1000 burst 256
Switch#
```

21-25 debug openflow meter-del

This command is used to simulate the OpenFlow OFPFC_DELETE message to delete a meter entry.

debug openflow meter-del {*NUM* **| all}**

Parameters

NUM	Specifies the meter ID. The range is from 1 to 4294901760.
all	Specifies to delete all meter entries.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to simulate the OpenFlow OFPFC_DELETE message to delete a meter entry.

Example

This example shows how to delete all meter entries.

```
Switch# debug openflow meter-del all
Switch#
```

22. Packet Debug Commands

22-1 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#
```

22-2 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=0x9f869ab8,total_size=432800,block_size=2148,
#   block_num=200,max_alloc=8,alloc_blocks=8 print count=8(input 0)
#9f869ac4------------------------------------------------------------------
0000: 01 80 c2 00 00 0e d0 ae  ec d9 9e 5e 81 00 00 01    ...........^....
0010: 88 cc 02 07 04 d0 ae ec  d9 9e 5e 04 06 07 31 2f    ..........^...1/
0020: 31 36 00 06 02 00 78 0a  00 0c 17 47 69 67 61 62    16....x....Gigab
0030: 69 74 20 45 74 68 65 72  6e 65 74 20 53 77 69 74    it Ethernet Swit
#9f86a338------------------------------------------------------------------
0000: 01 80 c2 00 00 0e d0 ae  ec d9 9e 5e 81 00 00 01    ...........^....
0010: 88 cc 02 07 04 d0 ae ec  d9 9e 5e 04 06 07 31 2f    ..........^...1/
0020: 31 36 00 06 02 00 78 0a  00 0c 17 47 69 67 61 62    16....x....Gigab
0030: 69 74 20 45 74 68 65 72  6e 65 74 20 53 77 69 74    it Ethernet Swit
#9f86abac------------------------------------------------------------------
0000: 01 80 c2 00 00 0e d0 ae  ec d9 9e 5e 81 00 00 01    ...........^....
0010: 88 cc 02 07 04 d0 ae ec  d9 9e 5e 04 06 07 31 2f    ..........^...1/
0020: 31 36 00 06 02 00 78 0a  00 0c 17 47 69 67 61 62    16....x....Gigab
0030: 69 74 20 45 74 68 65 72  6e 65 74 20 53 77 69 74    it Ethernet Swit
#9f86b420------------------------------------------------------------------
0000: 01 80 c2 00 00 0e d0 ae  ec d9 9e 5e 81 00 00 01    ...........^....
0010: 88 cc 02 07 04 d0 ae ec  d9 9e 5e 04 06 07 31 2f    ..........^...1/
0020: 31 36 00 06 02 00 78 0a  00 0c 17 47 69 67 61 62    16....x....Gigab
0030: 69 74 20 45 74 68 65 72  6e 65 74 20 53 77 69 74    it Ethernet Swit
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

22-3 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                 0-0           0-0    LACP_BPDU          0-0           0-0
BPDU               0-0           0-0    ARP                0-0           0-0
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    CFM                0-0           0-0
OAM_PDU            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    PTP_ETH            0-0           0-0
PTP_UDPv4          0-0           0-0    MPLS_ECHO          0-0           0-0
DDPv4              0-0           0-0    DDPv6              0-0           0-0
ISIS_PKT           0-0           0-0    Stacking           0-0           0-0
Total              0-0           0-0


Switch#
```

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.

23. Power over Ethernet (PoE) Commands (DGS-3630-28PC and DGS-3630-52PC Only)

23-1 poe pd description (Hybrid Mode Only)

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)#
```

23-2 poe pd legacy-support (Hybrid Mode Only)

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)#
```

23-3 poe pd priority (Hybrid Mode Only)

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 **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)#
```

23-4 poe policy preempt (Hybrid Mode Only)

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 policy preempt

no poe policy preempt

Parameters

None.

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 policy preempt
Switch(config)#
```

23-5 poe power-inline (Hybrid Mode Only)

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 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 command **no poe power-inline** 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)#
```

23-6 poe usage-threshold (Hybrid Mode Only)

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 usage-threshold *PERCENTAGE*

no poe usage-threshold *PERCENTAGE*

Parameters

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 usage-threshold 50
Switch(config)#
```

23-7 snmp-server enable traps poe (Hybrid Mode Only)

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

no snmp-server enable traps poe

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 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)#
```

23-8 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 interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

There are counters on ports to record the statistic and they can be shown by 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#
```

23-9 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}**

Parameters

INTERFACE-ID	(Optional) Specifies the interfaces to be displayed.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and 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.

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. If the interface ID is not specified with this command, then all PoE interfaces will be displayed. 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 doesn't 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, then the overload counter is increased.
Short	If the PD's internal circuit is shorted for some reason, then this counter is increased.
Power Denied	If the PoE software system decides to disallow providing power to the attached PD, then 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#
```

23-10 show poe power module

This command is used to display the setting and actual values of the power modules.

show poe power module [detail]

Parameters

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 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.

23-11 poe pd alive (Hybrid Mode Only)

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. *IP-ADDRESS* - Specifies the IPv4 address of the target PD.

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)#
```

23-12 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 separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User/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#
```

24. Power Saving Commands (Hybrid Mode Only)

24-1 dim led

This command is used to disable the port LED function. Use the **no** form of this command to restore the LED function.

dim led

no dim led

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to turn off the port LED function. Use the **no** form of the command to restore the LED function. When the port LED function is disabled, LEDs used to illustrate port status are all turned off to save power.

Example

This example shows how to disable the port LED function.

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

24-2 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 | length-detection | port-shutdown | dim-led | hibernation}

no power-saving {link-detection | length-detection | port-shutdown | dim-led | hibernation}

Parameters

link-detection	Specifies that power saving will be applied by link status.
length-detection	Specifies that power saving will be applied by cable length detection.
dim-led	Specifies that power saving will be applied by scheduled dimming LEDs.

port-shutdown	Specifies that power saving will be applied by scheduled port shutdown.
hibernation	Specifies that power saving will be applied by scheduled system hibernation. This feature can only be used when physical stacking 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 length detection is enabled, the device can reduce the power consumption of a port dependent on the detected cable length.

When dim LED is enabled, the device will turn off all the port's LEDs in the specified time range to save power.

When port shutdown is enabled, the device will shut off all ports in the specified time range to save power.

When Energy-Efficient Ethernet (EEE) is enabled, the device will activate EEE power saving for those EEE enabled ports.

When hibernation is enabled, the device will enter the hibernation mode in the specified time range to save power.

Example

This example shows how to enable power saving by shutting off the Switch's ports and toggle the Switch into the hibernation mode.

```
Switch# configure terminal
Switch(config)# power-saving port-shutdown
Switch(config)# power-saving hibernation
Switch(config)#
```

24-3 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.

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)#
```

24-4 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's LED will be turned off.

Example

This example shows how to add a time-range profile for the dim LED schedule.

```
Switch# configure terminal
Switch(config)# power-saving dim-led time-range off-duty
Switch(config)#
```

24-5 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)#
```

24-6 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)#
```

24-7 show power-saving

This command is used to display the power saving configuration information.

show power-saving [link-detection] [length-detection] [dim-led] [port-shutdown] [hibernation] [eee]

Parameters

link-detection	(Optional) Specifies to display the link detection state.
length-detection	(Optional) Specifies to display the cable length detection state.
dim-led	(Optional) Specifies to display the dim LED state.
port-shutdown	(Optional) Specifies to display the port shutdown state.
hibernation	(Optional) Specifies to display the hibernation state. This can only be displayed when physical stacking 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
Function Version: 3.00

Link Detection Power Saving
  State: Disabled

Length Detection Power Saving
  State: Disabled

Scheduled Hibernation Power Saving
  State: Disabled

Administrative Dim-LED
  State: Disabled

Scheduled Dim-LED Power Saving
  State: Disabled

Scheduled Port-shutdown Power Saving
  State: Disabled

EEE_Enabled Ports

Switch#
```

25. Protocol Independent Commands (Hybrid Mode Only)

25-1 ip route

This command is used to specify the next hop IPv4 address used in the default static route. Use the **no** form of this command to remove the next hop IPv4 address used in the default static route.

ip route *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS*

no ip route *NETWORK-PREFIX NETWORK-MASK IP-ADDRESS*

Parameters

NETWORK-PREFIX	Specifies the network address.
NETWORK-MASK	Specifies the network mask.
IP-ADDRESS	Specifies the IP address of the next hop that can be used to reach destination network.

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 static route. The Switch only supports the default static route.

Example

This example shows how to specify the next hop IPv4 address, 10.1.1.254, used in the default static route.

```
Switch# configure terminal
Switch(config)# ip route 0.0.0.0 0.0.0.0 10.1.1.254
Switch(config)#
```

25-2 ipv6 route

This command is used to specify the next hop IPv6 address used in the default static route. Use the **no** form of this command to remove the next hop IPv6 address used in the default static route.

ipv6 route default [*INTERFACE-ID***]** *NEXT-HOP-ADDRESS*

no ipv6 route default [*INTERFACE-ID***]** *NEXT-HOP-ADDRESS*

Parameters

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.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to specify the next hop IPv6 address used in the default static route.

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 default vlan1 fe80::0000:00ff:1111:2233
Switch(config)#
```

25-3 show ip route

This command is used to display the entry in the routing table.

show ip route [*PROTOCOL***]**

Parameters

PROTOCOL	(Optional) Specifies the routing protocol with the following keywords: **static** and **connected**.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the best routes that are currently at work.

Example

This example shows how to display the routing table.

```
Switch# show ip route
Code: C - connected, S - static
      * - candidate default

Gateway of last resort is 10.2.2.2 to network 0.0.0.0

S    0.0.0.0/0  via 10.2.2.2 ,vlan1
C    192.168.70.0/24 is directly connected, vlan1

Total Entries: 2

Switch#
```

25-4 show ipv6 route

This command is used to display the entry in routing table.

show ipv6 route [*PROTOCOL***] [database]**

Parameters

PROTOCOL	(Optional) Specifies the routing protocol with the following keywords: **static** and **connected**.
database	(Optional) Specifies to display all the related entries in the routing database instead of just the best route.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the best routes that are currently at work.

Example

This example shows how to display the routing entries for IPv6.

```
Switch# show ipv6 route

IPv6 Routing Table
Code: C - connected, S - static
      SLAAC - Stateless address autoconfiguration

C    2000:410:1::/64 [0/1] is directly connected, vlan1
S    ::/0 [1/1] via fe80::0000:00ff:1111:2233, vlan1

Total Entries: 2 entries, 2 routes
Switch#
```

26. Reboot Commands

26-1 reboot

This command is used to reboot the Switch.

reboot [unit *UNIT-ID* **[- | ,]] [force_agree]**

Parameters

Unit *UNIT-ID*	Specifies the unit ID to be configured.
,	(Optional) Specifies a series of unit IDs or separates a range of unit IDs from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of unit IDs. No space is allowed before or after the hyphen.
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...
```

26-2 reboot schedule

This command is used to configure a reboot schedule. Use the **no** form of this command to cancel the reboot schedule.

reboot schedule {in *MINUTES* **| at** *HH*:*MM* **[***DDMTHYYYY***]} [save_before_reboot]**

no reboot schedule

Parameters

in *MINUTES*	Specifies that the Switch should initiate a reboot after the time period specified here. The time value range is from 1 to 43200 minutes.
at	Specifies that the Switch should initiate a reboot at the specified date and time. The scheduled reboot must be initiated within 30 days
HH:*MM*	Enter the time at which the Switch should initiate the reboot.
DDMTHYYYY	(Optional) Enter the date at which the Switch should initiate the reboot. If the date is not specified, the Switch will initiate the reboot at the specified time on the current day if the specified time is later than the current time or on the next day if the specified time is earlier than the current time.
save_before_reboot	(Optional) Specifies that the Switch should save all the configurations made before initiating the reboot.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

Use **reboot schedule** command to start and configure the reboot schedule. After the Switch was rebooted, it will generate a log message to identify that the system was restarted using the reboot schedule.

The configuration file of the device will not include the **reboot schedule** command. After the reboot or shutdown, the reboot schedule will be deleted automatically. Moreover, if the Switch was manually rebooted or powered off before the reboot schedule takes effect, the specified reboot schedule will be cancelled.

Example

This example shows how to reboot the Switch in 10 minutes and save the configuration before the reboot.

```
Switch# reboot schedule in 10 save_before_reboot
Switch#
```

This example shows how to reboot the Switch on 27 March, 2021 at 11pm.

```
Switch# reboot schedule at 23:00 27mar2021
Switch#
```

26-3 show reboot schedule

This command is used to display the reboot schedule configuration.

show reboot schedule

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command is used to display the reboot schedule configuration.

Example

This example shows how to display the reboot schedule configuration.

```
Switch#show reboot schedule

 Reboot Schedule Settings
 ---------------------------
 Reboot scheduled at 27 Mar 2021 23:00:00 (in 520 minutes)
 Save before reboot: Yes


Switch#
```

27. Remote Network MONitoring (RMON) Commands (Hybrid Mode Only)

27-1 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)#
```

27-2 rmon collection history

This command is used to enable RMON MIB history statistics gathering on the configured interface. Use the **no** form of this command to disable history statistics gathering on the interface.

rmon collection history *INDEX* **[owner** *NAME***] [buckets** *NUM***] [interval** *SECONDS***]**

no rmon collection history *INDEX*

Parameters

INDEX	Specifies the history group table index. The range is from 1 to 65535.
owner *NAME*	Specifies the owner string. The maximum length is 127.
buckets *NUM*	Specifies the number of buckets specified for the RMON collection history group of statistics. If not specified, the default is 50. The range is from 1 to 65535.
interval *SECONDS*	Specifies the number of seconds in each polling cycle. The range is from 1 to 3600.

Default

By default, this option is disabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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)#
```

27-3 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 not specified, no action is taken while crossing the ringing threshold.
falling-threshold *VALUE*	Specifies the falling threshold. The valid range is from 0 to 2147483647.
FALLING-EVENT-NUMBER	(Optional) Specifies the index of the event entry that is used to notify the falling threshold crossing event. The valid range is from 1 to 65535. If not specified, no action is taken while crossing the falling threshold.
owner *STRING*	(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)#
```

27-4 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)#
```

27-5 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#
```

27-6 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#
```

27-7 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#
```

27-8 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#
```

27-9 snmp-server enable traps rmon

This command is used to enable the RMON trap state. Use the **no** form of this command to disable the state.

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 RMON trap state.

Example

This example shows how to enable the sending of RMON traps for both the falling alarm and rising alarm.

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

28. Secure File Transfer Protocol (SFTP) Server Commands (Hybrid Mode Only)

28-1 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)#
```

28-2 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)#
```

28-3 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#
```

29. Secure Shell (SSH) Commands

29-1 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#
```

29-2 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#
```

29-3 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)#
```

29-4 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 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)#
```

29-5 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)#
```

29-6 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 regarding the RSA public key.

```
Switch#show crypto key mypubkey rsa

% Key pair was generated at: 17:23:14, 2021-03-15
Key Size: 768 bits
Key Data:
AAAAB3Nz aC1yc2EA AAADAQAB AAAAYFeT JTzuNThG JS/Pk/Q3 uEuGY3vY Vk+Ap2kr
wtPhlvNT 6nf3355K yUSkoGkH fy962ZIH LkAL5U9U Aw90yUVY H/0SKyBE 72H2UpIT
GX+PbVyf /dOarjo/ +ST1vNYc j3CZmQ==

Switch#
```

29-7 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 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#
```

29-8 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 SSH connections' status on the Switch.

Example

This example shows how to display SSH connections' information.

```
Switch# show ssh

SID Ver. Cipher                      Userid           Client IP Address
--- --- ---------------------------- ---------------- -------------------------
0   V2  3des-cbc/hmac-sha1-96       zhang3           192.168.0.100
1   V2  3des-cbc/hmac-sha1          lee4567890123456 192.168.0.101

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.

29-9 ssh user authentication-method

This command is used to configure the SSH authentication method for a user account. Use the **no** form of this command to revert to the default settings.

ssh user *NAME* **authentication-method {password | publickey** *URL* **| hostbased** *URL* **host-name** *HOSTNAME* **[***IP-ADDRESS* **|** *IPV6-ADDRESS***]}**

no ssh user *NAME* **authentication-method**

Parameters

NAME	Specifies the username to configure the authentication type. The user must be an existing local account. The length of the username is limited to a maximum of 32 characters.
password	Specifies to use the password authentication method for this user account. This is the default authentication method.
publickey *URL*	Specifies to use the public key authentication method for this user account. Enter the URL of a local file to be used as the public key of this user.
hostbased *URL*	Specifies to use the host-based authentication method for this user account. Enter the URL of a local file to be used as client's host key.
host-name *HOSTNAME*	Specifies the allowed host name for host-based authentication. During authentication phase, the client's hostname will be checked. The range is from 1 to 255.
IP-ADDRESS	(Optional) Specifies whether to additionally check the IP address of the client for host-based authentication. If not specified, only the host name will be checked.
IPV6-ADDRESS	(Optional) Specifies whether to additionally check the IPv6 address of the client for host-based authentication. If not specified, only the host name will be checked. **(Hybrid Mode Only)**

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)#
```

30. Transport Layer Security (TLS) Commands

30-1 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 trust point. If the specified certificate is a local certificate the corresponding private key will be deleted at the same time.

Example

This example shows how to delete an imported certificate named *tongken.ca* of the trust point *gaa*.

```
Switch# show crypto pki trustpoints

Trustpoint Name        : gaa (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Switch# configure terminal
Switch(config)# crypto pki certificate chain gaa
Switch(config-cert-chain)# no certificate tongken.ca
Switch(config-cert-chain)#
```

30-2 crypto pki import pem

This command is used to import the CA certificate or the Switch certificate and keys to a trust-point from privacy-enhanced mail (PEM)-formatted files.

crypto pki import *TRUSTPOINT* **pem** *FILE-SYSTEM***:/[***DIRECTORY/***]***FILE-NAME* **[password** *PASSWORD-PHRASE***] {ca | local | both}**

crypto pki import *TRUSTPOINT* **pem tftp: //***IP-ADDRESS***[***DIRECTORY/***]** *FILE-NAME* **[password** *PASSWORD-PHRASE***] {ca | local | both}**

Parameters

TRUSTPOINT	Specifies the name of the trust-point that is associated with the imported certificates and key pairs.
FILE-SYSTEM	Specifies the file system for certificates and key pairs. A colon (:) is required after the specified file system.
DIRECTORY	(Optional) Specifies the directory name where the Switch should import the certificates and key pairs in the Switch or TFTP server.
FILE-NAME	Specifies the name of the certificates and key pairs to be imported. By default, the Switch will append this name with *.ca*, *.prv* and *.crt* for CA certificate, private key and certificate respectively.
password *PASSWORD-PHRASE*	(Optional) Specifies the encrypted password phrase that is used to undo encryption when the private keys are imported. The password phrase is a string of up to 64 characters. If the password phrase is not specified, the NULL string will be used.
tftp	Specifies the source URL for a TFTP network server.
IP-ADDRESS	Specifies the IP address of the TFTP server.
ca	Specifies to import the CA certificate only.
local	Specifies to import local certificate and key pairs only.
both	Specifies to import the CA certificate, local certificate and key pairs.

Default

None.

Command Mode

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 trust point CA is the certificate authority configured on the Switch as the trusted CA. Any obtained peer certificate will be accepted if it is signed by a locally trusted CA or its subordinates.

If the specified trust point doesn’t exist, an error message will be prompted.

Example

This example shows how to import certificates (CA and local) and key pair files to trust-point "TP1" via TFTP.

```
Switch# configure terminal
Switch(config)# crypto pki import TP1 pem tftp: //10.1.1.2/name/msca password abcd1234 both

% Importing CA certificate...
Destination filename [name/msca.ca]?
Reading file from tftp://10.1.1.2/name/msca.ca
Loading name/msca.ca from 10.1.1.2 (via 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)#
```

30-3 crypto pki trustpoint

This command is used to declare the trust-point that the Switch will use. Use the **no** form of this command to delete all certificates and key pairs associated with the trust-point.

crypto pki trustpoint *NAME*

no crypto pki trustpoint *NAME*

Parameters

NAME	Specifies to create a name for the trust-point.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to declare a trust-point, which can be a self-signed root certificate authority (CA) or a subordinate CA. Issuing this command will enter the CA-Trust-Point Configuration Mode.

Example

This example shows how to declare a trust-point "TP1" and specify it is a primary trust-point.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

30-4 crypto pki certificate chain

This command is used to enter into the certificate chain configuration mode.

crypto pki certificate chain *NAME*

Parameters

NAME	Specifies the name for the trust-point.

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to enter into certificate chain configuration mode. If the specified trust-point name doesn't exist, an error message will be displayed.

Example

This example shows how to enter into certificate chain configuration mode.

```
Switch# configure terminal
Switch(config)# crypto pki certificate chain TP1
Switch(trustpoint)#
```

30-5 primary

This command is used to assign a specified trust-point as the primary trust-point 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 trust-point as primary. This trust-point can be used as default trust-point when the application doesn't explicitly specify which certificate authority (CA) trust-point should be used. Only one trust-point can be specified as the primary. The last trust-point specified as the primary will overwrite the previous one.

Example

This example shows how to configure the trust-point "TP1" as the primary trust-point.

```
Switch# configure terminal
Switch(config)# crypto pki trustpoint TP1
Switch(ca-trustpoint)# primary
Switch(ca-trustpoint)#
```

30-6 show crypto pki trustpoints

This command is used to display the trust-points that are configured in the Switch.

show crypto pki trustpoints [*TRUSTPOINT***]**

Parameters

TRUSTPOINT	(Optional) Specifies the name of the trust-point to be displayed.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 12.

Usage Guideline

If no parameter is specified, all trust-points will be displayed.

Example

This example shows how to display all trust-points.

```
Switch# show crypto pki trustpoints

Trustpoint Name        : TP1 (primary)
  Imported certificates:
    CA                 : tongken.ca
    local certificate  : webserver.crt
    local private key  : webserver.prv

Trustpoint Name        : TP2
  Imported certificates:
    CA                 : chunagtel.ca
    local certificate  : openflow.crt
    local private key  : openflow.prv

Switch#
```

30-7 show ssl-service-policy

This command is used to display the SSL service policy.

show ssl-service-policy [*POLICY-NAME***]**

Parameters

POLICY-NAME	(Optional) Specifies the name of the SSL service policy.

Default

None.

Command Mode

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#
```

30-8 ssl-service-policy

This command is used to configure the SSL service policy. Use the **no** form of this command to remove the SSL service policy

ssl-service-policy *POLICY-NAME* **[version [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 applicance accepts TLS version 1.0. **tls1.1**- Indicate the applicance accepts TLS version 1.1. **tls1.2**- Indicate the applicance 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 trust-point that should be used in SSL handshake. When this parameter is not specified, the trust-point which is specified as the primary will be used. If no primary trust-point is specified, the built-in certificate/key pairs will be used. Use the **no** form of this command to cancel the specified trust-point 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” trust-point.

```
Switch# configure terminal
Switch(config)# ssl-service-policy ssl-server secure-trustpoint TP1
Switch(config)#
```

31. Simple Network Management Protocol (SNMP) Commands (Hybrid Mode Only)

31-1 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#
```

31-2 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#
```

31-3 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]**

no snmp-server community [0 | 7] *COMMUNITY-STRING*

Parameters

0 *COMMUNITY-STRING*	(Optional) Specifies the community string in the plain text form with a maximum of 32 alphanumeric characters. This is the default option.
7 *COMMUNITY-STRING*	(Optional) Specifies the community string in the encrypted form.
view *VIEW-NAME*	(Optional) Specifies a view name of a previously defined view. It defines the view accessible by the SNMP community.
ro	(Optional) Specifies read-only access.
rw	(Optional) Specifies read-write access.

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 the view is not specified, it is permitted to access all objects.

Example

This example shows how a MIB view “interfacesMibView” is created and a community string “comaccess” which can do read write access the interfacesMibView view is created.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server community comaccess view interfacesMibView rw
Switch(config)#
```

31-4 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 332200000000000000000000.

```
Switch# configure terminal
Switch(config)# snmp-server engineID local 3322
Switch(config)#
```

31-5 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, then Internet OID space 1.3.6.1 can be read.

The write-view defines the MIB objects that the group user is allowed to write. If write-view is not specified, then no MIB objects can be written.

The notification view defines the MIB objects that the system can report its status in the notification packets to the trap managers that are identified by the specified group user (act as community string). If notify-view is not specified, then no MIB objects can be reported.

Example

This example shows how to create the SNMP server group “guestgroup” for SNMPv3 access and SNMPv2c.

```
Switch# configure terminal
Switch(config)# snmp-server view interfacesMibView 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)# snmp-server group guestgroup v2c read CommunityView write CommunityView
Switch(config)#
```

31-6 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 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 or **snmp-server user v3** command.

In the sending of the trap packet, the system will check the notification view associated with the specified user (or community name). If the binding variables to be sent with the trap packet are not in the notification view, the notification will not be sent to this host.

Example

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with community string “comaccess”.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess
Switch(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 3 authentication security level and with the username “useraccess”.

```
Switch# configure terminal
Switch(config)# snmp-server group groupaccess v3 auth read CommunityView write CommunityView
Switch(config)# snmp-server user useraccess groupaccess v3 auth md5 12345678
Switch(config)# snmp-server host 163.10.50.126 version 3 auth useraccess
Switch(config)#
```

This example shows how to configure the trap recipient 163.10.50.126 with version 1 with the community string “comaccess”. The UDP port number is configured to 50001.

```
Switch# configure terminal
Switch(config)# snmp-server community comaccess rw
Switch(config)# snmp-server host 163.10.50.126 version 1 comaccess port 50001
Switch(config)#
```

31-7 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* **{v1| v2c | v3 [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* **{v1| v2c | v3}**

Parameters

USER-NAME	Specifies a username of a maximum of 32 characters. The syntax is general string that does not allow spaces.
GROUP-NAME	Specifies the name of the group to which the user belongs. The syntax is general string that does not allow spaces.
v1	Specifies that the user uses the SNMPv1 security mode.
v2c	Specifies that the user uses the SNMPv2c security mode.
v3	Specifies that the user uses the SNMPv3 security mode.
encrypted	(Optional) Specifies that the following password is in encrypted format.
auth	(Optional) Specifies the authentication level.
md5	(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 SMNP user, specify the security model that the user uses and the group that the user is created for. To create an SNMPv3 user, the password used for authentication and encryption needs to be specified.

An SNMP user is unable to be deleted if it has been associated with a SNMP server host.

Example

This example shows how 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 v3 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 v3 encrypted auth md5
00112233445566778899AABBCCDDEEFF
Switch(config)#
```

31-8 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 1.3.6.1.2.1.2 included
Switch(config)# snmp-server group guestgroup v3 auth read interfacesMibView
Switch(config)#
```

31-9 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#
```

31-10 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#
```

31-11 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#
```

31-12 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)#
```

31-13 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)#
```

31-14 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

This command enables the device to send the SNMP notification traps globally. To configure the router to send these SNMP notifications, enter the **snmp-server enable traps** command to enable the global setting.

Example

This example shows how to enable the SNMP traps global sending state.

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

31-15 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 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)#
```

31-16 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)#
```

31-17 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 and end with a letter or a digit and the interior characters can only contain 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
Switch(config)#
```

31-18 snmp-server trap-sending disable

This command is used to disable the port's trap sending state. Use the **no** form of this command to enable the port's trap sending state.

snmp-server trap-sending disable

no snmp-server trap-sending disable

Parameters

None.

Default

By default, this option is enabled.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command to disable the port to send SNMP notification traps out of the configured port. If the sending is disabled, then SNMP notification traps generated by the system are not allowed to transmit out of the port. The SNMP traps generated by other system and forwarded to the port is not subject to this restriction.

Example

This example shows how to disable the sending of the notification traps on port 8.

```
Switch# configure terminal
Switch(config)# interface eth1/0/8
Switch(config-if)# snmp-server trap-sending disable
Switch(config-if)#
```

31-19 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)#
```

31-20 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)#
```

31-21 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)#
```

32. Spanning Tree Protocol (STP) Commands (Hybrid Mode Only)

NOTE: STP cannot be enabled on OpenFlow enabled ports.

32-1 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#
```

32-2 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#
```

32-3 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	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 separate a range of instances from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of instances. No space is allowed before and after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the interface ID to be displayed.
,	(Optional) Specifies a series of interfaces, or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.
detai	(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#
```

32-4 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 separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

User/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#
```

32-5 snmp-server enable traps stp

This command is used to enable the spanning tree to send SNMP notifications for STP. Use the **no** form of 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. If no optional parameter is specified in the **no** form of this command, both STP notification types are disabled.

Example

This example shows how to enable the router to send all STP traps to the host 10.9.18.100 using the community string defined as public.

```
Switch# configure terminal
Switch(config)# snmp-server enable traps
Switch(config)# snmp-server enable traps stp
Switch(config)# snmp-server host 10.9.18.100 version 2c public
Switch(config)#
```

32-6 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)#
```

32-7 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 separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

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)#
```

32-8 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)#
```

32-9 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)#
```

32-10 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)#
```

32-11 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)#
```

32-12 spanning-tree global state

This command is used to enable or disable the STP's global state. Use the **no** form of this command to disable the STP's global state.

spanning-tree global state {enable | disable}

no spanning-tree global state

Parameters

enable	Specifies to enable the STP's global state.
disable	Specifies to disable the STP's global state.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use this command in the global configuration mode to enable the global spanning-tree function.

Example

This example shows how to enable the spanning-tree function.

```
Switch# configure terminal
Switch(config)# spanning-tree global state enable
Switch(config)#
```

32-13 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)#
```

32-14 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)#
```

32-15 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)#
```

32-16 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)#
```

32-17 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

The command is available for physical port and port-channel interfaces.

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)#
```

32-18 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)#
```

32-19 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)#
```

32-20 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)#
```

32-21 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)#
```

32-22 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)#
```

32-23 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 command **spanning-tree mst priority** to configure the priority for an MSTP instance.

Example

This example shows how to configure the STP bridge priority value to 4096.

```
Switch# configure terminal
Switch(config)# spanning-tree priority 4096
Switch(config)#
```

32-24 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)#
```

32-25 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)#
```

32-26 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)#
```

32-27 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)#
```

32-28 debug spanning-tree state

This command is used to enable or disable the spanning tree debugging function.

debug spanning-tree state {enable | disable}

Parameters

enable	Specifies to enable the spanning tree debugging function.
disable	Specifies to disable the spanning tree debugging function.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to enable or disable the spanning tree debugging function.

Example

This example shows how to enable the spanning tree debugging function.

```
Switch# debug spanning-tree state enable
Switch#
```

32-29 debug spanning-tree config

This command is used to configure the debugging level of the spanning tree on the specified interface(s).

debug spanning-tree config {all | bpdu | event | state_machine} state {brief | detail | disable} interface *INTERFACE-ID* **[, | -]**

Parameters

all	Specifies to debug BPDUs that have been received and transmitted, external operation and event processing, and the state change of the STP state machine.
bpdu	Specifies to debug the BPDUs that have been received and transmitted.

event	Specifies to debug the external operation and event processing.
state_machine	Specifies to debug the state change of the STP state machine.
state	Specifies the state of the debug level and mechanism. **brief** - Specifies to set the debug level to brief. **detail** - Specifies to set the debug level to detailed. **disable** - Specifies to disable the debug mechanism.
interface *INTERFACE-ID*	Specifies the interfaces to be used. **all** - Specifies to use all the port interfaces.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

By default, this function is disabled.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to configure the debugging level of the spanning tree on the specified interface(s).

Example

This example shows how to configure the debugging level of the spanning tree on port 1.

```
Switch# debug spanning-tree config state_machine state detail interface eth1/0/1
Switch#
```

32-30 debug spanning-tree clear counter

This command is used to clear the spanning tree debugging counter on the specified interface(s).

debug spanning-tree clear counter interface *INTERFACE-ID* **[, | -]**

Parameters

interface *INTERFACE-ID*	Specifies the interfaces to be used. **all** - Specifies to use all the port interfaces.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to clear the spanning tree debugging counter on the specified interface(s).

Example

This example shows how to clear the spanning tree debugging counter on port 1.

```
Switch# debug spanning-tree clear counter interface eth1/0/1
Switch#
```

32-31 debug spanning-tree show

This command is used to display the STP debugging information on the specified interface(s).

debug spanning-tree show {flag | counter} interface *INTERFACE-ID* **[, | -]**

Parameters

flag	Specifies to display the debugging level.
counter	Specifies to display the counter information.
interface *INTERFACE-ID*	Specifies the interfaces to be displayed. **all** - Specifies to use all the port interfaces.
,	(Optional) Specifies a series of interfaces or separate a range of interfaces from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before and after the hyphen.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the STP debugging information on the specified interface(s).

Example

This example shows how to display the STP debugging information on port 1.

```
Switch# debug spanning-tree show flag interface eth1/0/1

Global State: Disabled

Port Index       Event Flag       BPDU Flag       State Machine Flag
-------------------------------------------------------------
 1/0/1           Disabled         Disabled        Disabled

Switch#debug spanning-tree show counter interface eth1/0/1

  eth1/0/1
  Receive:                                  Transmit:
  Total STP Packets         : 0             Total STP Packets  : 0
  Configuration BPDU        : 0             Configuration BPDU : 0
  TCN BPDU                  : 0             TCN BPDU           : 0
  RSTP TC-Flag              : 0             RSTP TC-Flag       : 0
  RST BPDU                  : 0             RST BPDU           : 0

  Discard:
  Total Discarded BPDU      : 0
  Global STP Disabled       : 0
  Port STP Disabled         : 0
  Invalid packet Format     : 0
  Invalid Protocol          : 0
  Configuration BPDU Length : 0
  TCN BPDU Length           : 0
  RST BPDU Length           : 0
  Invalid Type              : 0
  Invalid Timers            : 0
Switch#
```

32-32 debug spanning-tree show information

This command is used to display the STP debugging information.

debug spanning-tree show information

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

Use this command to display the STP debugging information.

Example

This example shows how to display the STP debugging information.

```
Switch#debug spanning-tree show information

Warning: only support local device.
Spanning Tree Debug Information:
---------------------------------------
Port Status In Hardware Table:
Instance 0:
Port 1/0/1: FOR  Port 1/0/2: FOR  Port 1/0/3: FOR  Port 1/0/4: FOR  Port 1/0/5: FOR  Port
1/0/6: FOR
Port 1/0/7: FOR  Port 1/0/8: FOR  Port 1/0/9: FOR  Port 1/0/10: FOR  Port 1/0/11: FOR  Port
1/0/12: FOR
Port 1/0/13: FOR  Port 1/0/14: FOR  Port 1/0/15: FOR  Port 1/0/16: FOR  Port 1/0/17: FOR  Port
1/0/18: FOR
Port 1/0/19: FOR  Port 1/0/20: FOR  Port 1/0/21: FOR  Port 1/0/22: FOR  Port 1/0/23: FOR  Port
1/0/24: FOR
Port 1/0/25: FOR  Port 1/0/26: FOR  Port 1/0/27: FOR  Port 1/0/28: FOR  Port 1/0/29: FOR  Port
1/0/30: FOR
Port 1/0/31: FOR  Port 1/0/32: FOR  Port 1/0/33: FOR  Port 1/0/34: FOR  Port 1/0/35: FOR  Port
1/0/36: FOR
Port 1/0/37: FOR  Port 1/0/38: FOR  Port 1/0/39: FOR  Port 1/0/40: FOR  Port 1/0/41: FOR  Port
1/0/42: FOR
Port 1/0/43: FOR  Port 1/0/44: FOR  Port 1/0/45: FOR  Port 1/0/46: FOR  Port 1/0/47: FOR  Port
1/0/48: FOR
Port 1/0/49: FOR  Port 1/0/50: FOR  Port 1/0/51: FOR  Port 1/0/52: FOR
---------------------------------------
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

33. Switch Port Commands

33-1 duplex (Hybrid Mode Only)

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 | auto} [rj45 | sfp]

no duplex [rj45 | sfp]

Parameters

full	Specifies that the port operates in the full-duplex mode.
auto	Specifies that the port's duplex mode will be determined by auto-negotiation.
rj45	(Optional) Specifies to configure the duplex for RJ45 media. For combo ports, if RJ45 or SFP is not specified, RJ45 is implied.
sfp	(Optional) Specifies to configure the duplex for SFP media.

Default

The duplex mode will be set as automatic for 100BASE-TX and 1000BASE-T interfaces.

The duplex mode will be set as full for 100BASE-FX and 1000BASE-SX/LX interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

100BASE-FX is always set at the speed of 10 Mbps and full-duplex. 1000BASE-SX/LX is always set at the speed of 100 Mbps and full-duplex.

For 100BASE-FX and 1000BASE-SX/LX modules, this command cannot take effect.

Auto-negotiation will be enabled if either the speed parameter is set to auto or the duplex parameter is set to auto if the speed parameter is set to auto and the duplex parameter is set to the fixed mode only the speed will be negotiated. The advertised capability will be configured to the duplex mode combined with all the possible speeds. If the speed is to set to a fixed speed and duplex is set to auto, only the duplex mode is negotiated.

The half-duplex mode is not supported on the Switch.

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)#
```

33-2 flowcontrol (Hybrid Mode Only)

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)#
```

33-3 media-type (Hybrid Mode Only)

This command is used to configure the media of a combo port that is selected for connection. Use the **no** form of this command to revert to the default settings.

media-type {auto-select | rj45 | sfp}

no media-type

Parameters

auto-select	Specifies that the media is selected based on the user's connection.
rj45	Specifies to use RJ45 media for the connection, and SFP is disabled.
sfp	Specifies to use SFP media for the connection, and RJ45 is disabled.

Default

By default, this option is **auto-select**.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is only available for the combo ports.

Example

This example shows how to configure the media type to sfp on port 21.

```
Switch#configure terminal
Switch(config)#interface eth1/0/21
Switch(config-if)#media-type sfp
Switch(config-if)#
```

33-4 mdix (Hybrid Mode Only)

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)#
```

33-5 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 and 100Mbps.

speed {10 | 100 | 1000 [master | slave] | 10giga [master | slave] | auto [*SPEED-LIST*]} [rj45 | sfp]

no speed [rj45 | sfp]

Parameters

10	Specifies to force the speed to 10Mbps.
100	Specifies to force the speed to 100Mbps.
1000	Specifies that for copper ports, it forces the speed to 1000Mbps and the user must manually set that the port operates as master or slave. Specifies that for fiber ports (1000BASE-SX/LX), the port will disable the auto-negotiation.
master | slave	Specifies the port operates as master or slave timing. This parameter is only applicable to 1000BASE-T connections.
10giga	Specifies to force the speed to 10Gbps.
master | slave	Specifies the port operates as master or slave timing. This parameter is only applicable to 10GBASE-T connections.
auto	Specifies that for copper ports, it specifies to determine the speed and flow control via auto-negotiation with its link partner. Specifies that for fiber ports (1000BASE-SX/LX), it enables the auto-negotiation option. Auto-negotiation will start to negotiate the clock and flow control with its link partner.
SPEED-LIST	(Optional) Specifies a list of speeds that the Switch will only auto-negotiate to. The speed can be **1000**, and/or **10giga**. Use a comma (,) to separate multiple speeds. If the speed list is not specified, all speed will be advertised.
rj45	(Optional) Specifies to configure speed for RJ45 media. For combo ports, if RJ45 or SFP/SFP+ is not specified, RJ45 is used.
sfp	(Optional) Specifies to configure speed for SFP/SFP+ media.

Default

The speed is automatic for 100BASE-TX, 1000BASE-T and 10GBASE-T interfaces.

The speed is fixed to 100Mbps for 100BASE-FX interfaces.

The speed is fixed to 1000Mbps for 1000BASE-SX/LX interfaces.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

If the specified speed is not supported by the hardware, error messages will be returned. For the 100BASE-FX modules, the speed is always fixed at 100Mbps, full duplex, and no-negotiation. No command can change the settings. For the 1000BASE-SX/LX modules, the speed is always fixed to 1000Mbps and full duplex, and only the **speed 1000** and **speed auto** commands are valid. For a 1000BASE-T connection, if the speed is specified to 1000Mbps, the port must be configured as master or slave. For a 10GBASE-T connection, if the speed is specified to 10Gbps, the port must be configured as master or slave.

Auto-negotiation will be enabled when the speed parameter is set to **auto**. The advertised capability will be full duplex mode combined with the specified speeds. The half-duplex mode is not supported on the Switch.

For 10GBASE-R connections, if auto-negotiation is enabled, the system will automatically configure the speed (1000M or 10G) according to the type of SFP/SFP+.

Example

This example shows how to configure 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)#
```

33-6 speed auto-downgrade

This command is used to enable automatically downgrading advertised speed in case a link cannot be established at the available speed. Use the **no** form of this command to disable it.

speed auto-downgrade

no speed auto-downgrade

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 automatically downgrading advertised speed in case a link cannot be established at the available speed.

Example

This example shows how to enable speed auto-downgrade.

```
Switch#configure terminal
Switch(config)#interface eth1/0/5
Switch(config-if)#speed auto-downgrade
Switch(config-if)#
```

33-7 log link-status (Hybrid Mode Only)

This command is used to enable the log of the link status. Use the **no** form of this command to disable it.

log link-status

no log 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 only available for physical port interface configuration.

Use this command to enable the log of the link status.

Example

This example shows how to enable the log of the link status.

```
Switch#configure terminal
Switch(config)#interface eth1/0/2
Switch(config-if)#log link-status
Switch(config-if)#
```

---

34. System File Management Commands

34-1 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)#
```

34-2 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: 2.25.013
Description: D-Link Corporation Gigabit Ethernet Switch

Switch(config)#
```

This example shows how to checks a specified image file called “runtime.wrongswitch.had”. The checksum of the image file has been verified wrong and an error message is displayed.

```
Switch# configure terminal
Switch(config)# boot image check runtime.wrongswitch.had
ERROR: Invalid firmware image.
Switch(config)#
```

34-3 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#
```

34-4 reset system

This command is used to reset the system, clear the system's configuration, then save and reboot the Switch.

reset system

Parameters

None.

Default

None.

Command Mode

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...... 100 %


Please wait, the switch is rebooting...
```

34-5 configure replace

This command is used to replace the current running configuration with the indicated configuration file.

configure replace {{tftp: *//LOCATION/FILENAME* **| rcp:** *//USERNAME@LOCATION/FILENAME* **| ftp:** *//USERNAME*:*PASSWORD@LOCATION*:*TCPPORT/FILENAME* **| sftp:** *//LOCATION/FILENAME***} | flash:** *FILENAME***} [force]**

Parameters

tftp:	Specifies that the configuration file is from the TFTP server.
//LOCATION/FILENAME	Specifies the URL of the configuration file on the TFTP server.
rcp:	Specifies that the configuration file is from the RCP server.
//USERNAME@LOCATION/ FILENAME	Specifies the URL of the configuration file on the RCP server.
ftp:	Specifies that the configuration file is from the FTP server.
//USERNAME:*PASSWORD @LOCATION*:*TCPPORT/ FILENAME*	Specifies the URL of the configuration file on the FTP server.
sftp:	Specifies that the configuration file is from the SFTP server. The SFTP client settings must be configured before using this parameter.
//LOCATION/FILENAME	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 download the “config.cfg” from the RCP server and replace the current running configuration with it.

```
Switch#configure replace rcp: //User@10.0.0.66/config.cfg

This will apply all necessary additions and deletions
to replace the current running configuration with the
contents of the specified configuration file, which is
assumed to be a complete configuration, not a partial
configuration. [y/n]:  y

 Accessing rcp://10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to download the “config.cfg” from the FTP server and replace the current running configuration with it. Execute the command immediately without confirmation.

```
Switch# configure replace ftp: //User:123@10.0.0.66:80/config.cfg force

 Accessing ftp: //10.0.0.66/config.cfg...
 Transmission start...
 Transmission finished, file length 45422 bytes.
 Executing script file config.cfg ......
 Executing done

Switch#
```

This example shows how to replace the current running configuration with the specified configuration file “config.cfg” stored in the NVRAM of the device. Execute the command immediately without confirmation.

```
Switch# configure replace flash: config.cfg force

 Executing script file config.cfg ......
 Executing done

Switch#
```

34-6 copy

This command is used to copy a file to another file.

copy *SOURCE-URL DESTINATION-URL*

copy *SOURCE-URL* **{tftp: [**//*LOCATION*/*DESTINATION-URL*] **| ftp: [**//*USER-NAME*:*PASSWORD@LOCATION*:*TCP-PORT*/*DESTINATION-URL*] **| rcp: [**//*USER-NAME@LOCATION*/*DESTINATION-URL*] **| sftp: [**//*LOCATION*/*DESTINATION-URL*]}**

copy {tftp: [//*LOCATION*/*SOURCE-URL*] **| ftp: [**//*USER-NAME*:*PASSWORD@LOCATION*:*TCP-PORT*/*SOURCE-URL*] **| rcp: [**//*USER-NAME@LOCATION*/*SOURCE-URL*] **| sftp: [**//*LOCATION*/*SOURCE-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.
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/FTP/RCP/SFTP server.
USER-NAME	(Optional) Specifies the user name on the FTP/RCP server.
PASSWORD	(Optional) Specifies the password for the user.

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.

```
Switch#copy tftp: //192.168.1.123/2.25.013.had flash: image.had

Address of remote host [192.168.1.123]?
Source filename [2.25.013.had]?
Destination filename [image.had]?
 Accessing tftp://192.168.1.123/2.25.013.had...
 Transmission start...
 Transmission finished, file length 15478860 bytes.
 Please wait, programming flash.............. 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/dgs-3630.had flash: dgs-3630.had

Address of remote host [10.90.90.23]?
Source filename [dgs-3630.had]?
Destination filename [dgs-3630.had]?
 Start, aborted by CTRL+C or Esc, remote_file_path is dgs-3630.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.
 Wait slave programming flash complete...
 Done.

Switch#
```

34-7 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:/def_usr.cfg


Switch#
```

34-8 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. **(Hybrid Mode Only)**

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command displays the current running system configuration.

Example

This example shows how to display the content of the running configuration file.

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

Current configuration : 1507 bytes

!----------------------------------------------------------------------------
!                     DGS-3630-28PC Gigabit Ethernet Switch
!                                Configuration
!
!                             Firmware: Build 2.25.013
!           Copyright(C) 2021 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

aaa new-model
!
aaa group server radius group1
!
line console
 session-timeout 0
 login authentication default
!
line telnet
 login authentication default
!
line ssh
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

34-9 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-3630-28PC Gigabit Ethernet Switch
!                                Configuration
!
!                             Firmware: Build 2.25.013
!           Copyright(C) 2021 D-Link Corporation. All rights reserved.
!----------------------------------------------------------------------------

# AAA START
# AAA END
!
# COMMAND LEVEL START
# COMMAND LEVEL END
# LEVEL START
# LEVEL END
# ACCOUNT START
# ACCOUNT END
!
# LOGIN START
line console
 session-timeout 0
!
line telnet
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

35. System Log Commands

35-1 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#
```

35-2 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)#
```

35-3 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 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.

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)#
```

35-4 logging console

This command is used to enable the logging of system messages to the local console. Use the **no** form of this command to disable the logging of messages to the local console and revert to the default setting.

logging console [severity {*SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [discriminator** *NAME***]**

no logging console

Parameters

SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).

discriminator	(Optional) Specifies to filter the message to be sent to the local console based on the discriminator.

Default

By default, this option is disabled.

Command Mode

Global Configuration Mode.

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)#
```

35-5 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 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)#
```

35-6 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.
drops *STRING*	(Optional) Specifies to filter the matching message. Enter one or more facility names after the keyword. If multiple facility names are used, they should be separated by commas without spaces before and after the comma.
includes *STRING*	(Optional) Specifies to include the matching message. The unmatched messages are filtered. Enter one or more facility names after the keyword. If multiple facility names are used, they should be separated by commas without spaces before and after the comma.
severity	(Optional) Specifies a sub-filter based on severity matching.
drops *SEVERITY-LIST*	(Optional) Specifies to filter the matching message. Enter the list of severity levels to be filtered after the keyword.

includes *SEVERITY-LIST*	(Optional) Specifies to include the matching message. The unmatched messages are filtered. Enter the list of severity levels to be included after the keyword.

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 PORT severity includes
1-4,6
Switch(config)#
```

35-7 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. **(Hybrid Mode Only)**
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If not specified, the default severity level is warnings (**4**).
SEVERITY-NAME	(Optional) Specifies the severity level name of system messages. The corresponding severity levels are listed together with their respective severity names: **emergencies** (0), **alerts** (1), **critical** (2), **errors** (3), **warnings** (4), **notifications** (5), **informational** (6), **debugging** (7).

FACILITY-NUM	(Optional) Specifies a decimal value from 0 to 23 to represent the facility. If not specified, the default facility is local7 (**23**). See the usage guideline for more information.
FACILITY-NAME	(Optional) Specifies a facility name to represent the facility. If not specified, the default facility is **local7** (23). See the usage guideline for more information.
discriminator *NAME*	(Optional) Specifies to filter the message to the log server based on discriminator.
port *UDP-PORT*	(Optional) Specifies the UDP port number to be used for the SYSLOG server. Valid values are 514 (the IANA well-known port) or any value from 1024 to 65535. If not specified, the default UDP port is 514.

Default

None.

Command Mode

Global Configuration Mode.

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)#
```

35-8 show logging

This command is used to display the system messages logged in the local message buffer.

show logging [all | [*REF-SEQ***] [+** *NN* **| -** *NN***]]**

Parameters

all	(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:4

#4     2021-03-15 16:01:58 CRIT(2) System started up
#3     2021-03-15 16:01:58 CRIT(2) System warm start
#2     2021-03-15 15:59:42 CRIT(2) System started up
#1     2021-03-15 15:59:42 CRIT(2) System warm start

Switch#
```

36. Time and SNTP Commands

36-1 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#
```

36-2 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)#
```

36-3 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)#
```

36-4 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          : 05:56:45, 2000-01-30
     Time Zone             : UTC +00:00
     Daylight Saving Time  : Disabled

Switch#
```

36-5 show sntp (Hybrid Mode Only)

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::1111vlan1                                ------- ---------------
---------------------------------------------- ------- ---------------

Total Entries:3

Switch#
```

36-6 sntp server (Hybrid Mode Only)

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)#
```

36-7 sntp enable (Hybrid Mode Only)

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)#
```

36-8 sntp interval (Hybrid Mode Only)

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)#
```

37. Time Range Commands (Hybrid Mode Only)

37-1 periodic

This command is used to specify the period of time for a time range profile. This command is used in the time-range configuration mode. 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)#
```

37-2 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#
```

37-3 time-range

This command is used to define a time-range profile and enter the time range configuration mode. 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)#
```

38. Virtual LAN (VLAN) Commands

38-1 acceptable-frame (Hybrid Mode Only)

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)#
```

38-2 ingress-checking (Hybrid Mode Only)

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)#
```

38-3 show vlan

This command is used to display the parameters for all configured VLANs or one VLAN on the Switch.

show vlan [*VLAN-ID* **[, | -] | interface [***INTERFACE-ID* **[, | -]]]**

Parameters

VLAN-ID	(Optional) Specifies a list of VLANs to display the member port information. If the VLAN is not specified, all VLANs are displayed. The valid range is from 1 to 4094.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.
interface *INTERFACE-ID*	(Optional) Specifies the physical port or port-channel interface to display the VLAN related setting. Port-channel interface is only available in the hybrid mode.
,	(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 parameters for all configured VLANs or one VLAN on the Switch.

Example

This example shows how to display all the current VLAN entries.

```
Switch#show vlan

 VLAN 1
   Name : default
   Description :
   Tagged Member Ports   :
   Untagged Member Ports : eth1/0/1-1/0/28

 Total Entries : 1

Switch#
```

This example shows how to display the PVID, ingress checking, and acceptable frame type information for ports 1 to 3.

```
Switch# show vlan interface eth1/0/1-3

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

Switch#
```

38-4 switchport access vlan

This command is used to specify the access VLAN for an interface. Use the **no** form of this command to revert to the default setting.

switchport access vlan *VLAN-ID*

no switchport access vlan

Parameters

VLAN-ID	Specifies the access VLAN of the interface.

Default

By default, this access VLAN is VLAN 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

The command takes effect when the interface is set to access mode. The VLAN specified as the access VLAN does not need to exist to configure the command.

Only one access VLAN can be specified. The succeeding command overwrites the previous command.

Example

This example shows how to configure port 1 to access mode with access VLAN 1000.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1000
Switch(config-if)#
```

38-5 switchport hybrid allowed vlan

This command is used to specify the tagged or untagged VLANs for a hybrid port. Use the **no** form of this command to revert to the default setting.

switchport hybrid allowed vlan {[add] {tagged | untagged} | remove} *VLAN-ID* **[, | -]**

no switchport hybrid allowed vlan

Parameters

add	(Optional) Specifies the port will be added into the specified VLAN(s).
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 option is specified, the specified VLAN list will overwrite the allowed VLAN list.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, a hybrid port is an untagged member port of VLAN 1.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

By setting the hybrid VLAN command multiple times with different VLAN IDs, a port can be a tagged member port or an untagged member port of multiple VLANs.

When the allowed VLAN is only specified as the VLAN ID, the succeeding command will overwrites the previous command. If the new untagged allowed VLAN list is overlap with the current tagged allowed VLAN list, the overlap part will change to the untagged allowed VLAN. On the other hand, if the new tagged allowed VLAN list is overlap with current untagged allowed VLAN list, the overlap part will change to the tagged allowed VLAN. The last command will take effect. The VLAN does not need to exist to configure the command.

Example

This example shows how to configure 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)#
```

38-6 switchport hybrid native vlan

This command is used to specify the native VLAN ID of a hybrid port. Use the **no** form of this command to revert to the default setting.

switchport hybrid native vlan *VLAN-ID*

no switchport hybrid native vlan

Parameters

VLAN-ID	Specifies the native VLAN of a hybrid port.

Default

By default, the native VLAN of a hybrid port is VLAN 1.

Command Mode

Interface Configuration Mode.

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)#
```

38-7 switchport mode

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

switchport mode {access | hybrid | trunk}

no switchport mode

Parameters

access	Specifies the port as an access port.
hybrid	Specifies the port as a hybrid port.
trunk	Specifies the port as a trunk port.

Default

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

Command Mode

Interface Configuration Mode.

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.

When a port is set to trunk mode, this port is either a tagged or untagged member port of its native VLAN and can be a tagged member of other VLANs configured. The purpose of a trunk port is to support the switch-to-switch connection.

When the switch-port mode is changed, the VLAN related setting associated with previous mode will be lost.

Example

This example shows how to configure port 1 as a trunk port.

```
Switch# configure terminal
Switch(config)# interface eth1/0/1
Switch(config-if)# switchport mode trunk
Switch(config-if)#
```

38-8 switchport trunk allowed vlan

This command is used to configure the VLANs that are allowed to receive and send traffic on the specified interface in a tagged format. Use the **no** form of this command to revert to the default setting.

switchport trunk allowed vlan {all | [add | remove | except] *VLAN-ID* **[, | -]}**

no switchport trunk allowed vlan

Parameters

all	Specifies that all VLANs are allowed on the interface.
add	Specifies to add the specified VLAN list to the allowed VLAN list.
remove	Specifies to remove the specified VLAN list from the allowed VLAN list.
except	Specifies that all VLANs except the VLANs in the exception list are allowed.
VLAN-ID	Specifies the allow VLAN list or the VLAN list to be added to or removed from the allow VLAN list.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

By default, all VLANs are allowed.

Command Mode

Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command only takes effect when the interface is set to trunk mode. If a VLAN is allowed on a trunk port, the port will become the tagged member of the VLAN. When the allowed VLAN option is set to **all**, the port will be automatically added to all the VLAN created by the system.

Example

This example shows how to configure 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)#
```

38-9 switchport trunk native vlan

This command is used to specify the native VLAN ID of a trunk mode interface. Use the **no** form of this command to revert to the default setting.

switchport trunk native vlan {*VLAN-ID* **| tag}**

no switchport trunk native vlan [tag]

Parameters

VLAN-ID	Specifies the native VLAN for a trunk port.
tag	Specifies to enable the tagging mode of the native VLAN.

Default

By default, the native VLAN is 1, untagged mode.

Command Mode

Interface Configuration Mode.

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)#
```

38-10 vlan

This command is used to add VLANs and enter the VLAN configuration mode. Use the **no** form of this command to remove VLANs.

vlan *VLAN-ID* **[, | -]**

no vlan *VLAN-ID* **[, | -]**

Parameters

VLAN-ID	Specifies the ID of the VLAN to be added, removed or configured. The valid VLAN ID range is from 1 to 4094. VLAN ID 1 cannot be removed.
,	(Optional) Specifies a series of VLANs, or separate a range of VLANs from a previous range. No space is allowed before and after the comma.
-	(Optional) Specifies a range of VLANs. No space is allowed before and after the hyphen.

Default

The VLAN ID 1 exists in the system as the default VLAN.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

Use the **vlan** global configuration command to create VLANs. Entering the **vlan** command with a VLAN ID enters the VLAN configuration mode. Entering the VLAN ID of an existing VLAN does not create a new VLAN, but allows the user to modify the VLAN parameters for the specified VLAN. When the user enters the VLAN ID of a new VLAN, the VLAN will be automatically created.

Use the **no vlan** command to remove a VLAN. The default VLAN cannot be removed. If the removed VLAN is a port's access VLAN, the port's access VLAN will be reset to VLAN 1.

Example

This example shows how to add new VLANs, assigning the new VLANs with the VLAN IDs 1000 to 1005.

```
Switch# configure terminal
Switch(config)# vlan 1000-1005
Switch(config-vlan)#
```

38-11 name

This command is used to specify the name of a VLAN. Use the **no** form of this command to revert to the default setting.

name *VLAN-NAME*

no name

Parameters

VLAN-NAME	Specifies the VLAN name, with a maximum of 32 characters. The VLAN name must be unique within the administrative domain.

Default

The default VLAN name is VLANx, where x represents four numeric digits (including the leading zeros) that are equal to the VLAN ID.

Command Mode

VLAN Configuration Mode.

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)#
```

Appendix A - Password Recovery Procedure

This section describes the procedure for resetting passwords on the D-Link DGS-3630 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                                          V2.00.002
-------------------------------------------------------------------------------

  Power On Self Test ....................................  100 %

  MAC Address    : F0-7D-68-30-36-00
  H/W Version    : A1

  Please Wait, Loading 2.25.013 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.

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. 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.	Warning
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. vid: The assign VLAN ID that authorized by from RADIUS server. interface-id: It indicates the port number of the client authenticated. username: It indicates the username for authentication.	Informational
Event Description: 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.	Warning

interface-id: It indicates the port number of the client authenticated. acl-script: The assign ACL script that authorized by from RADIUS server.	

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. ipif_name: The name of the interface of the switch which has the conflict IP address.	Warning

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>) 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: 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.	Informational

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 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. 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 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.	Informational

serverIP: Server IP address. pathFile: Path and file name on server.	
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: 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: Represent current login user. ipaddr: Represent client IP address.	Informational
Event description: Configuration saved to flash by console. Log Message: [Unit <unitID>,]System log saved to flash by console (Username: <username>) Parameters description: unitID: The unit ID. username: Represent current login user.	Informational
Event description: Configuration saved to flash by remote. Log Message: [Unit <unitID>,]System log saved to flash (Username: <username>, IP: <ipaddr>) Parameters description: unitID: The unit ID. username: Represent current login user. ipaddr: Represent 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, and SSH 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.

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

Interface

Log Description	Severity
Event Description: Port link up. Log Message: Port <portNum> link up, <link state> Parameters Description: portNum: 1.Interger value;2.Represent the logic port number of the device. link state: for ex: , 100Mbps FULL duplex.	Informational
Event Description: Port link down. Log Message: Port <portNum> link down Parameters Description: portNum: 1.Interger value;2.Represent the logic port number of the device.	Informational

LACP

Log Description	Severity
Event Description: Link Aggregation Group link up. Log Message: Link Aggregation Group <group_id> link up Parameters Description: group_id: The group id of the link up aggregation group.	Informational
Event Description: Link Aggregation Group link down. Log Message: Link Aggregation Group <group_id> link down Parameters Description: group_id: The group id of the link down aggregation group.	Informational
Event Description: Member port attach to Link Aggregation Group. Log Message: <ifname> attach to Link Aggregation Group <group_id> Parameters Description: Ifname: The interface name of the port that attach to aggregation group. group_id: The group id of the aggregation group that port attach to.	Informational
Event Description: Member port detach from Link Aggregation Group. Log Message: <ifname> detach from Link Aggregation Group <group_id> Parameters Description: Ifname: The interface name of the port that detach from aggregation group. group_id: The group id of the aggregation group that port detach from.	Informational

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:	Warning

unitID: The unit ID. username: Represent current login user.	
Event Description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Login through Telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through Telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Critical
Event Description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational

Parameters Description:
username: Represent current login user.
ipaddr: Represent client IP address.

MSTP Debug

Log Description	Severity
Event Description: Topology changed. Log Message: Topology changed [([Instance:<InstanceID>] , <portNum> ,MAC: <macaddr>)] Parameters Description: InstanceID: Instance ID. portNum: Port ID. macaddr: MAC address.	Notification
Event Description: Spanning Tree new Root Bridge. Log Message: [CIST | CIST Regional | MSTI Regional] New Root bridge selected ([Instance: <InstanceID>],MAC: <macaddr>, Priority:<value>) Parameters Description: InstanceID: Instance ID. macaddr: Mac address. value: priority value.	Informational
Event Description: Spanning Tree Protocol is enabled. Log Message: Spanning Tree Protocol is enabled	Informational
Event Description: Spanning Tree Protocol is disabled. Log Message: Spanning Tree Protocol is disabled	Informational
Event Description: New root port. Log Message: New root port selected [([Instance:<InstanceID>], <portNum>)] Parameters Description: InstanceID: Instance ID. portNum: Port ID.	Notification
Event Description: Spanning Tree port status changed. Log Message: Spanning Tree port status change [([Instance:<InstanceID>], <portNum>)] <old_status> -> <new_status> Parameters Description: InstanceID: Instance ID. portNum: Port ID. old_status: new_status: The port of STP state. The value may be Disable, Discarding, Learning, Forwarding.	Notification
Event Description: Spanning Tree port role changed. Log Message: Spanning Tree port role change. [([Instance:<InstanceID>], <[portNum>)] <old_role> -> <new_role> Parameters Description: InstanceID: Instance ID. portNum: Port ID. old_role: new_status: The port role of stp. The value may be DisabledPort, AlternatePort, BackupPort, RootPort, DesignatedPort, MasterPort.	Informational

Event Description: Spanning Tree instance created. Log Message: Spanning Tree instance created. (Instance:<InstanceID>) Parameters Description: InstanceID: Instance ID.	Informational
Event Description: Spanning Tree instance deleted. Log Message: Spanning Tree instance deleted. (Instance:<InstanceID>) Parameters Description: InstanceID: Instance ID.	Informational
Event Description: Spanning Tree Version changed. Log Message: Spanning Tree version change.(New version:<new_version>) Parameters Description: new_version: New STP version.	Informational
Event Description: Spanning Tree MST configuration ID name and revision level changed. Log Message: Spanning Tree MST configuration ID name and revision level change (name:<name> revision level <revision_level>) Parameters Description: name: New name. revision_level: New revision level.	Informational
Event Description: Spanning Tree MST configuration ID VLAN mapping table deleted. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> delete vlan <startvlanid> [- <endvlanid>]) Parameters Description: InstanceID: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
Event Description: Spanning Tree MST configuration ID VLAN mapping table added. Log Message: Spanning Tree MST configuration ID VLAN mapping table change (instance: <InstanceID> add vlan <startvlanid> [- <endvlanid>]) Parameters Description: InstanceID: Instance ID. startvlanid-endvlanid: VLAN list.	Informational
Event Description: Spanning Tree port role change to alternate port due to the guard root. Log Message: Spanning Tree port role change (Instance: <InstanceID>, <portNum>) to alternate port due to the guard root Parameters Description: InstanceID: Instance ID. portNum: Port ID.	Informational
Event Description: Spanning Tree loop guard blocking. Log Message: Spanning Tree loop guard blocking(Instance: <InstanceID>, <portNum>) Parameters Description: InstanceID: Instance ID. portNum: Port ID.	Informational

OpenFlow

Log Description	Severity
Event Description: This log will be generated when OpenFlow TCP session is successfully connected with the controller.	Informational

Log Message: TCP session is successfully connected with the controller <ipaddr>:<port> Parameters Description: ipaddr: It indicates the controller's IP address. port: It indicates the L4 port number.	
Event Description: This log will be generated when OpenFlow TCP session is disconnected from the controller. Log Message: TCP session is disconnected from the controller <ipaddr>:<port> Parameters Description: ipaddr: It indicates the controller's IP address. port: It indicates the L4 port number.	Informational
Event Description: This log will be generated when flow setting from controller is failed. Log Message: Flow entry (cookie is <cookie>) setting <set-type> from the controller is failed. Parameters Description: cookie: The cookie is specified by the controller when the flow is installed. set-type: It indicates the flow entry settings. The types include: • OFPFC_ADD • OFPFC_MODIFY • OFPFC_MODIFY_STRICT • OFPFC_DELETE • OFPFC_DELETE_STRICT	Error
Event Description: This log will be generated when the flow entry is deleted by the controller. Log Message: Flow entry cookie <cookie> is deleted by controller <ipaddr>:<port> Parameters Description: cookie: The cookie is specified by the controller when the flow is installed. ipaddr: It indicates the controller's IP address. port: It indicates the L4 port number.	Warning
Event Description: This log will be generated when the flow entry is deleted because of idle time, hard timeout expire, flow-mod request, and overwrite. Log Message: Flow entry cookie <cookie> is deleted because of <delete-reason> Parameters Description: cookie: The cookie is specified by the controller when the flow is installed. delete-reason: It indicates the reason to delete the flow entry. It contains: • "idle timeout (<duration> seconds)" • "hard timeout (<duration> seconds)" • "FLOW_MOD request" • "overwrite" <duration> indicates the value of timeout.	Warning
Event Description: This log will be generated when the flow setting from the controller failed. Log Message: An error <error-type> occurs with the controller <ipaddr> Parameters Description: error-type: It indicates the error type when an error occurs between the Switch and the controller. The error type may be: • OFPET_BAD_REQUEST • OFPET_FLOW_MOD_FAILED • OFPET_GROUP_MOD_FAILED • OFPET_ROLE_REQUEST_FAILED • OFPET_METER_MOD_FAILED ipaddr: It indicates the controller's IP address.	Error

Peripheral

Log Description	Severity
Event Description: Fan Recovered. Log Message: Unit <unit-id>, <fan-descr> back to normal Parameters Description: Unit <id>: The unit ID. <fan-descr>: For example, right fan, left fan etc.	Critical
Event Description: Fan Fail. Log Message: Unit <unit-id> <fan-descr> failed Parameters Description: Unit <id>: The unit ID. <fan-descr>: For example, right fan, left fan etc.	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: Description of the sensor. degree: The current temperature of the sensor.	Warning
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: Description of the sensor. degree: The current temperature of the sensor.	Informational
Event Description: Power failed. Log Message: Unit <unit-id> <power-descr> failed Parameters Description: Unit <id>: The unit ID. power-descr: Describe the power.	Critical
Event Description: Power is recovered. Log Message: Unit <unit-id> <power-descr> back to normal Parameters Description: Unit <id>: The unit ID. power-descr: Describe the power.	Critical
Event Description: External Alarm state to change. Log Message: Uint <unit-id> External Alarm Channel <channelID>:<alarmMsg> Parameters Description: Unit <id>: The unit ID. channelID: The channel ID. alarmMsg: The alarm Msg.	Critical

PoE

Log Description	Severity
Event Description: Total power usage threshold is exceeded. Log Message: Unit <unit-id> usage threshold <percentage> is exceeded	Warning

Parameters Description: unit-id: The box ID. percentage: Usage threshold.	
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

Log Description	Severity
Event Description: Port linkup. Log Message: Port <port> link up, <nway> Parameters Description: port: Represents the logical port number. nway: Represents the speed and duplex of link.	Informational
Event Description: Port link down. Log Message: Port <port> link down Parameters Description: port: Represents the logical port number.	Informational

Reboot Schedule

Log Description	Severity
Event Description: Tips is about will to reboot switch within the specified time. Log Message: Display "Reboot scheduled in 5 minutes" when the countdown equals 5 minutes	Warning
Event Description: Tips is about will to reboot switch within the specified time. Log Message: Display "Reboot scheduled in 1 minute" when the countdown equals 1 minute	Critical
Event Description: after schedule reboot in a specific interval. Log Message: System was restarted by schedule in an interval time	Informational
Event Description: after schedule reboot at specific time. Log Message: System was restarted by schedule at specific time	Informational
Event Description: after schedule reboot happens with save_before_reboot configured. Log Message: Configuration was saved by schedule	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

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

Web

Log Description	Severity
Event Description: Successful login through Web. Log Message: Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational

Parameters Description: username: The use name that used to login HTTP server. ipaddr: The IP address of HTTP client.	
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 HTTPS server. ipaddr: The IP address of HTTPS client.	Informational
Event Description: Login failed through Web (SSL). Log Message: Login failed through Web(SSL) (Username: <username>, IP: <ipaddr>) Parameters Description: username: The use name that used to login HTTPS server. ipaddr: The IP address of HTTPS 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 HTTPS server. ipaddr: The IP address of HTTPS 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 HTTPS server. ipaddr: The IP address of HTTPS client.	Informational

Appendix C - Trap Entries

The following table lists all possible trap log entries and their corresponding meanings that will appear in the Switch.

Authentication Fail

Trap Name	Description	OID
authenticationFailure	An authenticationFailure trap signifies that the SNMPv2 entity, acting in an agent role, has received a protocol message that is not properly authenticated. While all implementations of the SNMPv2 must be capable of generating this trap, the snmpEnableAuthenTraps object indicates whether this trap will be generated.	1.3.6.1.6.3.1.1 .5.5

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

External Alarm

Trap Name	Description	OID
dExternalAlarmStatusChg	The commander switch will send this notification when External alarm state is changed. Binding objects: (1) dExternalAlarmUnitID (2) dExternalAlarmChannel (3) dExternalAlarmStatus	1.3.6.1.4.1.17 1.14.32.0.1

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 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 .5.4
linkDown	A linkDown trap signifies that the SNMP entity, acting in an agent role, has detected that the ifOperStatus object for one of its communication links is about to enter the down state from some other state (but not from the notPresent state). This other state is indicated by the included value of ifOperStatus. Binding objects: (1) ifIndex (2) ifAdminStatus (3) ifOperStatus	1.3.6.1.6.3.1.1 .5.3

MAC Notification

Trap Name	Description	OID
dL2FdbMacNotification	This trap indicate the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfo	1.3.6.1.4.1.17 1.14.3.0.1
dL2FdbMacNotificationWithVID	This trap indicate the MAC addresses variation in the address table. Binding objects: (1) dL2FdbMacChangeNotifyInfoWithVID	1.3.6.1.4.1.17 1.14.3.0.2

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 sent by a bridge soon after its election as the new root, e.g., upon expiration of the Topology Change Timer, immediately subsequent to its election. Implementation of this trap is optional.	1.3.6.1.2.1.17. 0.1
topologyChange	A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same transition. Implementation 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	1.3.6.1.4.1.17 1.14.5.0.1
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	1.3.6.1.4.1.17 1.14.5.0.2
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	1.3.6.1.4.1.17 1.14.5.0.3

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. Binding objects: (1) pethMainPseConsumptionPower	1.3.6.1.2.1.10 5.0.2
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	1.3.6.1.2.1.10 5.0.3
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	1.3.6.1.4.1.17 1.14.24.0.1
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	1.3.6.1.4.1.17 1.14.24.0.2

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	1.3.6.1.4.1.17 1.14.24.0.3
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.	1.3.6.1.4.1.17 1.14.24.0.4

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

Reboot Schedule

Trap Name	Description	OID
agentRebootIn5Min	This trap is sent when the countdown equals 5 minutes.	1.3.6.1.4.1.17 1.14.170.0.1
agentRebootIn1Min	This trap is sent when the countdown equals1 minute.	1.3.6.1.4.1.17 1.14.170.0.2

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.	1.3.6.1.2.1.16. 0.2

	Binding objects: (1) alarmIndex (2) alarmVariable (3) alarmSampleType (4) alarmValue (5) alarmFallingThreshold

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

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

Upload/Download

Trap Name	Description	OID
agentFirmwareUpgrade	This trap is sent when the process of upgrading the firmware via SNMP has finished. Binding objects: (1) swMultiImageVersion	1.3.6.1.4.1.17 1.12.1.7.2.0.7
agentCfgOperCompleteTrap	The trap is sent when the configuration is completely saved, uploaded or downloaded. Binding objects: (1) unitID (2) agentCfgOperate (3) agentLoginUserName	1.3.6.1.4.1.17 1.12.1.7.2.0.9

Appendix D - OpenFlow Object Details

Application developers can program a set of objects in the Switch using the OpenFlow protocol (version 1.3). The programmable objects include Flow Tables, Group Table entries, and Meter Table entries. This section provides programming descriptions for these objects.

Flow Table

Flow Table Number Assignments

Flow Table Name	Flow Table ID	Default Table Miss Action
Policy ACL Flow Table	0	Drop

Flow Table Counters

Field	Description
Reference Count (Active Entries)	Reference count of number of active entries in the table.
Packet Lookups	Not supported.
Packet Matches	Not supported.

Policy ACL Flow Table

Policy ACL Flow Table Match Fields

Field	Description
IN_PORT	The input port on the Switch.
IN_PHY_PORT	The physical input port on the Switch.
ETH_DST	The Ethernet destination address. **Note:** IPv6 flow (ETH_TYPE=0x86DD) is not supported.
ETH_SRC	The Ethernet source address. **Note:** IPv6 flow (ETH_TYPE=0x86DD) is not supported.
ETH_TYPE	The Ethernet frame type. **Note:** The Policy ACL Flow Table is organized into two mutually exclusive logical sub-tables. The flow entries in the IPv6 logical tables match only IPv6 packets (ETH_TYPE=0x86DD). The non-IPv6 logical table matches any non-IPv6 packets (ETH_TYPE≠0x86DD or when the ETH_TYPE is not specified).
VLAN_VID	The VLAN ID. **Note:** This must be programmed with 0x1000 (OFPVID_PRESENT).
VLAN_PCP	The VLAN priority.
IP_DSCP	The IP DSCP (6 bits in the ToS field).
IP_PROTO	The IP protocol.
IPV4_SRC	The source IPv4 address.
IPV4_DST	The destination IPv4 address.
TCP_SRC	The source TCP port.
TCP_DST	The destination TCP port.
UDP_SRC	The source UDP port.

UDP_DST	The destination UDP port.
SCTP_SRC	The source SCTP port.
SCTP_DST	The destination SCTP port.
ARP_SPA	The ARP source IPv4 address.
IPV6_SRC	The source IPv6 address.
IPV6_DST	The destination IPv6 address.

Policy ACL Flow Table Instructions

Field	Description
Write-Actions	Only the actions in the **Policy ACL Flow Table Action Set** table can be specified.
Apply-Actions	Only the actions in **Policy ACL Flow Table Action List Actions** table can be specified.
Clear-Actions	This is used to clear the action set.
Goto-Table	Not supported.
Write-Metadata	Not supported.
Meter	Specifies to apply the indicated meter. The meter entry must exist before the flow is installed.

Policy ACL Flow Table Action List Actions

Field	Description
Output	This sets the output port. It supports physical ports and the reserved controller port.
Set-Field	This supports VLAN_PCP, IP_ECN and IP_DSCP fields.

Policy ACL Flow Table Action Set

Field	Description
Group	This sets the output group entry for processing the packet after this table. The group must exist, be consistent with the type of rule and packet, and can be any of the following: • a Layer 2 interface group entry, • a Layer 2 rewrite group entry, • a Layer 2 multicast group entry, • a Layer 3 unicast group entry, and • a Layer 3 ECMP group entry.

Policy ACL Flow Table Counters

Field	Description
Received Packets	The number of packets that is received by this flow entry.
Received Bytes	The number of bytes that is received by this flow entry.
Duration (Seconds)	The time, in seconds, since this flow entry was installed.

Restrictions:

This Policy ACL Flow Table is organized into two mutually exclusive logical sub-tables. One is used to match IPv6 flows and the other one is used to match non-IPv6 flows. These two tables should be considered as a single table. But there are some restrictions:

- IPv6 packets might match two rules in the Policy ACL Flow table. It is recommended add ETH_TYPE or other Match Fields in the non-IPv6 logical table to avoid this issue.
- The same meter cannot be applied to two rules in different sub-tables. It is recommended to apply different meters for different rules to avoid this issue.

Group Table

L2 Interface Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the **L2 Interface Group Entry Naming Conversion** table.
Group Type	Indirect.
Counters	Specifies per-group entry counters.
Action Buckets	Supports a single action bucket.

L2 Interface Group Entry Naming Conversion

Field	Bits	Description
Interface ID	0 to 15	The interface ID.
Chain ID	16 to 27	The ID that other group type entries chain to. The range is from 1 to 4094.
Kind	28 to 31	0 (L2 Interface).

L2 Interface Group Entry Bucket Actions

Field	Description
Output	Supported on physical ports only.

L2 Interface Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed.

L2 Rewrite Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the **L2 Rewrite Group Entry Naming Conversion** table.
Group Type	Indirect.

Counters	Specifies per-group entry counters.
Action Buckets	Supports a single action bucket.

L2 Rewrite Group Entry Naming Conversion

Field	Bits	Description
ID	0 to 27	This is the index to differentiate between group entries of this type.
Kind	28 to 31	1 (L2 Rewrite).

L2 Rewrite Group Entry Bucket Actions

Field	Description
Group	This required field must be chained to a Layer 2 interface group entry.
Set-Field	This optional field sets the ETH_DST, ETH_SRC, and VLAN_VID fields.

L2 Rewrite Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed.

L2 Multicast Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the **L2 Multicast Group Entry Naming Conversion** table.
Group Type	All.
Counters	Specifies per-group entry counters.
Action Buckets	Supports multiple action buckets.

L2 Multicast Group Entry Naming Conversion

Field	Bits	Description
Index	0 to 15	This is the index to these kind of groups.
Chain ID	16 to 27	The chain ID is used to reference to Layer 2 interface group entries. The range is from 1 to 4094.
Kind	28 to 31	3 (L2 Multicast).

L2 Multicast Group Entry Bucket Actions

Field	Description
Group	This must chain to a Layer 2 interface group entry whose chain ID name component matches the chain ID component of this group entry's name.

L2 Multicast Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed.

L3 Unicast Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the **L3 Unicast Group Entry Naming Conversion** table.
Group Type	Indirect.
Counters	Specifies per-group entry counters.
Action Buckets	Supports a single action bucket.

L3 Unicast Group Entry Naming Conversion

Field	Bits	Description
ID	0 to 27	This is the index to differentiate between group entries of this type.
Kind	28 to 31	2 (L3 Unicast).

L3 Unicast Group Entry Bucket Actions

Field	Description
Group	This required field must be chained to a Layer 2 interface group entry.
Decrement TTL	The decremented TTL. **Note:** The check for invalid TTLs is not supported.
Set-Field	This required field sets the ETH_DST, ETH_SRC, and VLAN_ID fields.

L3 Unicast Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed

L3 ECMP Group Entry Type

Field	Description
Group Identifier	A 32-bit unsigned integer, uniquely identifying the group on the OpenFlow switch. The naming rule is shown in the **L3 ECMP Group Entry Naming Conversion** table.
Group Type	Select.
Counters	Specifies per-group entry counters.
Action Buckets	Supports multiple action buckets.

L3 ECMP Group Entry Naming Conversion

Field	Bits	Description
ID	0 to 27	This is used to differentiate between Layer 3 ECMP group entries.
Kind	28 to 31	7 (L3 ECMP).

L3 ECMP Group Entry Bucket Actions

Field	Description
Group	This is chained to a Layer 3 unicast group entry.

L3 ECMP Group Entry Counters

Field	Description
Reference Count (Flow Entries)	The number of flow entries or group entries that are currently referencing this group entry.
Duration (Seconds)	The time, in seconds, since this group entry was installed

Meter Table

Meter Table Entry Parameters

Field	Description
Meter Identifier	The meter instance.
Flags	The bit position: • **0:** Kbps (Kbps and Packets cannot be used at the same time). • **1:** Packets (Kbps and Packets cannot be used at the same time). • **2:** Burst (Required). • **3:** Stats (Not supported).
Meter Bands	Only one meter band is supported.
Counters	Specifies per-meter entry counters.

Meter Entry Counters

Field	Description
Flow Count	The number of flow entities that are currently referencing to this meter table entry.
Input Packet Count	Not supported.
Input Byte Count	Not supported.
Duration (Seconds)	The time, in seconds, since this meter table entry was installed.

Meter Band Configuration Parameters

Field	Description
Band Type	Only the Drop band type is supported
Rate	This is used by the meter to select the meter band. It defines the lowest rate applied to the band.
Burst	This defines the granularity of the meter band.
Counters	Not supported.