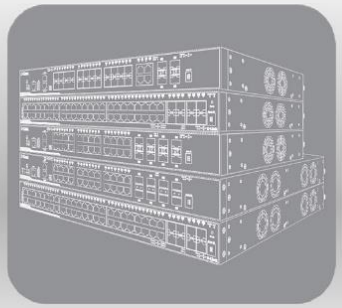
D-Link
Building Networks for People



CLI Reference Guide

Product Model: DGS-3630 Series

Layer 3 Stackable Managed Switch

Release 2.10 (OpenFlow)

Table of Contents

1. Introduction

This manual's command descriptions are based on the software release **2.10**, 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 either from the CD, bundled with this switch, or from the D-Link website. Other documents related to this switch are:

- *DGS-3630 Series Hardware Installation Guide*
- *DGS-3630 Series Command Line Interface (CLI) Guide (Legacy)*

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 2.10.012
                 Copyright(C) 2018 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) Specify the unit to display.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

```
Switch#show unit

Unit         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 2018  14:57:12 - 9  Apr 2018  14:42:12  : 14  %
9  Apr 2018  14:42:12 - 9  Apr 2018  14:27:12  : 14  %
9  Apr 2018  14:27:12 - 9  Apr 2018  14:12:12  : 14  %
9  Apr 2018  14:12:12 - 9  Apr 2018  13:57:12  : 14  %
9  Apr 2018  13:57:12 - 9  Apr 2018  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:2.10.012


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 2018  14:25:28 - 10 Apr 2018  14:10:28  : 39  %
10 Apr 2018  14:10:28 - 10 Apr 2018  13:55:28  : 39  %
10 Apr 2018  13:55:28 - 10 Apr 2018  13:40:28  : 39  %
10 Apr 2018  13:40:28 - 10 Apr 2018  13:25:28  : 39  %
10 Apr 2018  13:25:28 - 10 Apr 2018  13:10:28  : 39  %

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 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)#
```

3-3 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)#
```

3-4 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)#
```

3-5 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)#
```

3-6 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)#
```

3-7 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)#
```

3-8 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)#
```

3-9 show terminal

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

show terminal

Parameters

None.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

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

Example

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

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

Switch#
```

3-10 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 Anonymous       15        12M53S

Total Entries: 1

Switch#
```

3-11 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#
```

3-12 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)#
```

3-13 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)#
```

3-14 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 #
```

3-15 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)#
```

3-16 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)#
```

3-17 banner exec

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

banner exec *cMESSAGEc*

no banner exec

Parameters

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

Default

None.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

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

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

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

Example

This example shows how to configure an 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)#
```

3-18 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)#
```

3-19 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. Authentication, Authorization, and Accounting (AAA) Commands

4-1 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 to disable the accounting service.

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)#
```

4-2 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 to disable the accounting service.

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)#
```

4-3 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 to disable the accounting service.

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)#
```

4-4 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)#
```

4-5 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)#
```

4-6 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)#
```

4-7 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+)#
```

4-8 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)#
```

4-9 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)#
```

4-10 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)#
```

4-11 clear aaa counters servers

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

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

Parameters

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

tacacs all	Specifies to clear server counter information related to all TACACS hosts.
sg *NAME*	Specifies to clear server counter information related to all hosts in a server group.

Default

None.

Command Mode

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#
```

4-12 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)#
```

4-13 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)#
```

4-14 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)#
```

4-15 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* **[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.
auth-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending authentication packets. The range is 0 to 65535. Set the port number to zero if the server host is not for authentication purposes. The default value is 1812.
acct-port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending accounting packets. The range is 0 to 65535. Set the port number to zero if the server host is not for accounting purposes. The default value is 1813.
timeout *SECONDS*	Specifies the server time-out value. The range of timeout is between 1 and 255 seconds. If not specified, the default value is 5 seconds.
retransmit *COUNT*	(Optional) Specifies the retransmit times of requests to the server when no response is received. The value is from 0 to 20. Use 0 to disable the retransmission. If not specified, the default value is 2
0	(Optional) Specifies the password in clear text form. This is the default option.
7	(Optional) Specifies the password in the encrypted form.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can between 1 and 254 clear text characters.

Default

By default, no server is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

```
Switch#configure terminal
Switch(config)# radius-server host 172.19.10.100 auth-port 1500 acct-port 1501 timeout 8
retransmit 3 key ABCDE
Switch(config)# radius-server host 172.19.10.101 auth-port 1600 acct-port 1601 timeout 3
retransmit 1 key ABCDE
Switch(config)#
```

4-16 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*

no server *IP-ADDRESS*

Parameters

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

Default

By default, no server is configured.

Command Mode

RADIUS Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

4-17 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*

no server *IP-ADDRESS*

Parameters

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

Default

By default, no host is in the server group.

Command Mode

TACACS+ Group Server Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

4-18 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#
```

4-19 tacacs-server host

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

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

no tacacs-server host *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IPv4 address of the TACACS+ server.
port *PORT-NUMBER*	(Optional) Specifies the UDP destination port number for sending request packets. The default port number is 49. The range is 1 to 65535.
timeout *SECONDS*	(Optional) Specifies the time-out value. This value must be between 1 and 255 seconds. The default value is 5 seconds.
0	(Optional) Specifies the password in the clear text form. This is the default option.
7	(Optional) Specifies the password in the encrypted form.
key *KEY-STRING*	Specifies the key used to communicate with the server. The key can be from 1 to 254 clear text characters.

Default

No TACACS+ server host is configured.

Command Mode

Global Configuration Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

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

4-20 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.

4-21 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.

5. Basic IPv4 Commands

5-1 ip address

This command is used to configure the IP address for the management interface. Use the **no** command to remove the IP address from the management interface.

ip address *IP-ADDRESS SUBNET-MASK*

no ip address *IP-ADDRESS SUBNET-MASK*

Parameters

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

Default

By default, the IP address is 192.168.0.1 and subnet mask is 255.255.255.0.

Command Mode

MGMT Interface Configuration Mode.

Command Default Level

Level: 12.

Usage Guideline

This command is used to configure the IP address for the management interface.

Example

This example shows how to configure the IP address for the management interface to 10.108.1.27/8.

```
Switch# configure terminal
Switch(config)# interface mgmt0
Switch(config-if)# ip address 10.108.1.27 255.0.0.0
Switch(config-if)#
```

5-2 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)#
```

5-3 show ip interface

This command is used to display the IP interface information.

show ip interface [mgmt *ID***] [brief]**

Parameters

mgmt *ID*	(Optional) Specifies to display information related to the out-of-band management port interface. The ID can only be 0.
brief	(Optional) Specifies to display a summary of the IP interface information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

If no parameter is specified, information for all the interfaces will be displayed.

Example

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

```
Switch#show ip interface

mgmt_ipif 0  is enabled, Link status is down
  IP Address is 192.168.0.1/24
  Gateway is 0.0.0.0

Total Entries: 1

Switch#
```

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

```
Switch#show ip interface brief


Interface    IP Address      Link Status
----------  ---------------  -----------
mgmt_ipif   192.168.0.1      down

Total Entries: 1

Switch#
```

6. Command Logging Commands

6-1 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)#
```

7. CPU Port Statistics Commands

7-1 debug show cpu port

This command is used to display statistics for Layer 2 or Layer 3 control packets that are trapped to the CPU.

debug show cpu port [l2 | l3 [unicast | multicast] | protocol *NAME***]**

Parameters

l2	(Optional) Specifies to display statistic counters of Layer 2 control packets.
l3	(Optional) Specifies to display statistic counters of Layer 3 control packets.
unicast	(Optional) Specifies to display statistic counters of Layer 3 unicast routing and Layer 3 application control packets.
multicast	(Optional) Specifies to display statistic counters of Layer 3 multicast routing control packets.
protocol *NAME*	(Optional) Specifies the name of protocol. It is case sensitive.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is use to display statistics for Layer 2 and Layer 3 control packets that are trapped to the CPU.

Example

This example shows how to display all Layer 2 and Layer 3 protocol control packets that are trapped to the CPU.

```
Switch#debug show cpu port

Type                              PPS         Total       Drop
--------------------------------- ----------- ----------- -----------
802.1X                            0           0           0
ARP                               0           0           0
BGP                               0           0           0
CFM                               0           0           0
CTP                               0           0           0
DHCP                              0           0           0
DHCPv6                            0           0           0
DNS                               0           0           0
DVMRP                             0           0           0
ERPS                              0           0           0
GVRP                              0           0           0
ICMP                              0           0           0
ICMPv6                            0           0           0
IGMP                              0           0           0
ISIS                              0           0           0
LACP                              0           0           0
LLDP                              0           0           0
MLD                               0           0           0
NDP                               0           0           0
OAM                               0           0           0
OSPFv2                            0           0           0
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

7-2 debug clear cpu port

This command is used to reset all counters for Layer 2 or Layer 3 control packets that are trapped to the CPU.

debug clear cpu port

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to reset all counters for Layer 2 or Layer 3 control packets that are trapped to the CPU.

Example

This example shows how to clear all statistics counters.

```
Switch# debug clear cpu port
Switch#
```

8. Debug Commands

8-1 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)#
```

8-2 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#
```

8-3 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)#
```

8-4 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#
```

8-5 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#
```

8-6 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#
```

8-7 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#
```

8-8 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#
```

8-9 debug show tech-support

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

debug show tech-support

Parameters

None.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

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

```
Switch#debug show tech-support

#------------------------------------------------------------------------------
#                     DGS-3630-28PC Gigabit Ethernet Switch
#                         Technical Support Information
#
#                           Firmware: Build 2.10.012
#    Copyright(C) 2018  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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

[SYS 2018-3-15 17:11:49]

Boot Time           : 15 Mar 2018  16:00:48
RTC Time            : 2018/03/15 17:11:49
Boot PROM Version   : Build 2.10.001
Firmware Version    : Build 2.10.012
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
```

8-10 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
```

9. File System Commands

9-1 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 2018 15:54:55  runtime.had
2   -rw      15466640 Mar 13 2018 14:51:40  firmware.had
3   -rw          3088 Apr 11 2018 15:47:01  config.cfg
4   -rw      15478860 Mar 21 2018 14:06:29  fw5.had
5   d--             0 Apr 11 2018 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#
```

9-2 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#
```

9-3 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#
```

9-4 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#
```

9-5 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#
```

9-6 more

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

more *FILE-URL*

Parameters

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

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

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

Example

This example shows how to display the contents of file “usr_def.conf”.

```
Switch# more  /c:/configuration/usr_def.conf

!DGS-3630
!Firmware Version: 2.10.012
!Slot      Model
!------ ------------------
! 1        DGS-3630-28TC
! 2        -
! 3        DGS-3630-28TC
! 4        DGS-3630-28TC
!
!.
end

Switch#
```

9-7 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#
```

9-8 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#
```

9-9 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.

10. Interface Commands

10-1 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 ports.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

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#
```

10-2 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)#
```

10-3 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.
- **mgmt** - Specifies the Ethernet interface used for the out-of-band management port.

The format of the interface number is dependent on the interface type.

For physical port interfaces, the user cannot enter the interface if the Switch port does not exist. The physical port interface cannot be removed by the **no** command.

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)#
```

10-4 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)#
```

10-5 show counters

This command is used to display interface information.

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

Parameters

interface *INTERFACE-ID*	(Optional) Specifies the physical port interface to be displayed. If no interface is specified, counters of all interfaces will be displayed.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the statistic counters for an interface.

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                      : 2766
txHCTotalPkts                      : 0
rxHCUnicastPkts                    : 0
txHCUnicastPkts                    : 0
rxHCMulticastPkts                  : 668
txHCMulticastPkts                  : 0
rxHCBroadcastPkts                  : 2098
txHCBroadcastPkts                  : 0
rxHCOctets                         : 348696
txHCOctets                         : 0
rxHCPkt64Octets                    : 2077
rxHCPkt65to127Octets               : 200
rxHCPkt128to255Octets              : 27
rxHCPkt256to511Octets              : 402
rxHCPkt512to1023Octets             : 60
rxHCPkt1024to1518Octets            : 0
rxHCPkt1519to1522Octets            : 0
rxHCPkt1519to2047Octets            : 0
rxHCPkt2048to4095Octets            : 0
rxHCPkt4096to9216Octets            : 0
txHCPkt64Octets                    : 0
txHCPkt65to127Octets               : 0
txHCPkt128to255Octets              : 0
txHCPkt256to511Octets              : 0
txHCPkt512to1023Octets             : 0
txHCPkt1024to1518Octets            : 0
txHCPkt1519to1522Octets            : 0
txHCPkt1519to2047Octets            : 0
txHCPkt2048to4095Octets            : 0
txHCPkt4096to9216Octets            : 0

rxCRCAlignErrors                   : 0
rxUndersizedPkts                   : 0
rxFragmentPkts                     : 0
rxSymbolErrors                     : 0
rxDropPkts                         : 2766

txCollisions                       : 0
ifInErrors                         : 0
ifOutErrors                        : 0
ifInDiscards                       : 2766
ifOutDiscards                      : 0
txDelayExceededDiscards            : 0
txCRC                              : 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).
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).
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.
rxDropPkts	Packets dropped caused by destination port bitmap is 0 with ingress logic.

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, 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.
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.

10-6 show interfaces

This command is used to display the interface information.

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

Parameters

INTERFACE-ID	(Optional) Specifies that the interface can be a physical port, VLAN, loopback interface, or other.

,	(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 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#
```

10-7 show interfaces counters

This command is used to display counters on specified interfaces.

show interfaces [*INTERFACE-ID* **[, | -]] counters [errors | history {15_minute [slot 1-5] | 1_day [slot 1-2]}]**

Parameters

INTERFACE-ID	(Optional) Specifies the physical port interfaces to be displayed. If no interface is specified, counters of all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
errors	(Optional) Specifies to display the error counters.

history	(Optional) Specifies to display the history counters. If this parameter is specified, the historical statistics counters will not be displayed.
15_minute	(Optional) Specifies to display the 15-minute-based statistics count.
1_day	(Optional) Specifies to display the daily-based statistics count.

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 : 9  Apr 2018  14:51:06
Endtime   : 9  Apr 2018  14:36:06
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
```

10-8 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
```

10-9 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 1-5] | 1_day [slot 1-2]}]**

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, the utilization of all physical port interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional)Specifies a range of interfaces. No space is allowed before or after the hyphen.
utilization	(Optional) Specifies to display the utilization information.
history	(Optional) Specifies to display the historical interfaces utilization information. If this parameter is specified, the historical utilization for interfaces will not be displayed.
15_minute	(Optional) Specifies to display the 15-minute-based statistics count.
1_day	(Optional) Specifies to display the daily-based statistics count.

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 2018  14:56:13 - 9  Apr 2018  14:41:13  : 0   %
9  Apr 2018  14:41:13 - 9  Apr 2018  14:26:13  : 0   %
9  Apr 2018  14:26:13 - 9  Apr 2018  14:11:13  : 0   %
9  Apr 2018  14:11:13 - 9  Apr 2018  13:56:13  : 0   %
9  Apr 2018  13:56:13 - 9  Apr 2018  13:41:13  : 0   %

Switch#
```

10-10 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#
```

10-11 show interfaces description

This command is used to display the description and link status of interfaces.

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

Parameters

INTERFACE-ID	(Optional) Specifies the interface ID. If no interface is specified, then information related to all interfaces will be displayed.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.
description	Specifies to display the description and link status of interfaces.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

This command 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
```

10-12 shutdown

This command is used to disable an interface. Use the **no** form of this command to enable an interface.

shutdown

no shutdown

Parameters

None.

Default

By default, this option is **no shutdown**.

Command Mode

Interface Configuration Mode.

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)#
```

11. IP Utility Commands

11-1 ping

This command is used to diagnose basic network connectivity.

ping [ip] *IP-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.
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#
```

12. Jumbo Frame Commands

12-1 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)#
```

13. OpenFlow Commands

13-1 openflow global enable

This command is used to enable the OpenFlow function. Use the **no** 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.

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...
```

13-2 openflow controller

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

openflow controller *IP-ADDRESS* **[service-port** *TCP-PORT***]**

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.

Default

By default, the TCP port number is 6653 and 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 TCP port number of 6666.

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

13-3 openflow table-miss

This command is used to configure the table-miss entry. Use the **no** 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)#
```

13-4 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.

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. This command is only available when the OpenFlow function is globally enabled.

Example

This example shows how to clear the statistics information from the flow entry with the cookie ID of 0x64.

```
Switch# clear openflow statistics cookie 0x64
Switch#
```

13-5 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 State       : Enabled
OpenFlow Mode        : Pure
OpenFlow Ports       : 1/0/1-1/0/3

OpenFlow Controller  :
IP address      Port  Connection Role   Status
--------------- ----- ---------- ------ ------
192.168.55.101  6553  TCP        Equal  Up
192.168.55.102  6653  TCP        Master Down
192.168.55.103  6653  TCP        Slave  Down

Total Entries: 3

Switch#
```

13-6 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. This command is only available when the OpenFlow function is globally enabled.

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  = 2048
    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

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  = 2048
    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

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.

13-7 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 only available when the OpenFlow function is globally enabled.

Example

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

```
Switch# show openflow flows
------------------------------------------------------------------------------
Set time: 2018-03-15 14:6:41, cookie=0x100009D0EC495, table=0, n_packets=0, n_bytes=0,
idle_timeout=0, hard_timeout=0, priority=5, etherType:mask=0x0800:0xFFFF,
actions=outputPort:CONTROLLER(Reserved), drop
Set time: 2018-03-15 14:6:41, cookie=0x1000011AC6475, table=0, n_packets=0, n_bytes=0,
idle_timeout=0, hard_timeout=0, priority=5, etherType:mask=0x0806:0xFFFF,
actions=outputPort:CONTROLLER(Reserved), drop
Set time: 2018-03-15 14:6:41, cookie=0x10000E990E1D1, table=0, n_packets=0, n_bytes=0,
idle_timeout=0, hard_timeout=0, priority=40000, etherType:mask=0x0806:0xFFFF,
actions=outputPort:CONTROLLER(Reserved), drop
Set time: 2018-03-15 14:6:41, cookie=0x100002C9C719B, table=0, n_packets=0, n_bytes=0,
idle_timeout=0, hard_timeout=0, priority=40000, etherType:mask=0x88CC:0xFFFF,
actions=outputPort:CONTROLLER(Reserved), drop
Set time: 2018-03-15 14:6:41, cookie=0x100004C7F6023, table=0, n_packets=0, n_bytes=0,
idle_timeout=0, hard_timeout=0, priority=40000, etherType:mask=0x8942:0xFFFF,
actions=outputPort:CONTROLLER(Reserved), drop


Switch#
```

13-8 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. This command is only available when the OpenFlow function is globally enabled.

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#
```

13-9 debug openflow

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

debug openflow [connection | event]

no debug openflow [connection | event]

Parameters

connection	(Optional) Specify to display the connection type debug log.
event	(Optional) Specify 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#
```

14. Packet Debug Commands

14-1 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#
```

14-2 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
```

14-3 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.

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

15-1 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#
```

15-2 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#
```

This example shows how to display the PoE power inline LLDP classification.

```
Switch# show poe power-inline lldp-classification

Interface eth1/0/1
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 25.0W
PSE allocated power value: 25.0W

Interface eth1/0/2
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: high
PD requested power value: 0.0W
PSE allocated power value: 0.0W

Information from PD:

none

Interface eth1/0/3
PSE TX information:

Power type; type 2 PSE
Power source: primary power source
Power priority: low
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Information from PD:

Power type: type 2 PD
Power source: PSE
Power priority: unknown
PD requested power value: 20.0W
PSE allocated power value: 20.0W

Switch#
```

Display Parameters

Interface	The PoE interface ID.

Power type	The power type field which is in the Power via MDI TLV from PSE or PD LLDP packet.
Power source	The power source field which is in the Power via MDI TLV from PSE or PD LLDP packet.
Power priority	The power priority field which is in the Power via MDI TLV from PSE or PD LLDP packet.
PD requested power value	The PD requested power value field which is in the Power via MDI TLV from PSE or PD LLDP packet.
PSE allocated power value	The PSE allocated power value field which is in the Power via MDI TLV from PSE or PD LLDP packet.

15-3 show poe power module

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

show poe power module [unit *UNIT-ID***] [detail]**

Parameters

unit *UNIT-ID*	(Optional) Specifies the stacking unit's ID to be configured. This parameter is only available, if stacking is enabled.
detail	(Optional) Specifies to display more detailed chip parameter information.

Default

None.

Command Mode

User/Privileged EXEC Mode.

Command Default Level

Level: 1.

Usage Guideline

Use this command to display the detailed power information and PoE chip parameters for PoE modules.

Example

This example shows how to display the setting and actual values of the power modules.

```
Switch#show poe power module

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
-------------------------------------------------------------------------------
1      0             370               50              Enabled    Enabled

Switch#
```

Display Parameters

Unit	The unit ID of stacking device.
Delivered	The actual amount of power delivered to the PD in watts.
Power budget	The total power can be provided by the device in watts.
Usage-Threshold	The utilization threshold to record a log.
Preempt	**Enabled:** The power management mode is policy preempt, high priority PD can preempt the provided power of lower priority PD. **Disabled:** The power management mode is first in first serviced.
Trap State	**Enabled:** The trap is sent when the PoE usage threshold exceeds the specified value. **Disabled:** The trap is not sent when the PoE usage threshold exceeds the specified value.

Example

This example shows how to display the PoE detailed parameters for unit 1.

```
Switch#show poe power module unit 1 detail

Unit Delivered(W)  Power Budget(W)  Usage-Threshold(%)   Preempt   Trap State
-------------------------------------------------------------------------
1      0             370               50              Enabled    Enabled

PoE system parameters:
Unit   Max Ports   Device ID    SW Version
----   ---------   ---------    ----------
1      24          E121         20

Switch#
```

Display Parameters

Max ports	The maximum port number of the PoE sub-system.
Device ID	The hardware version of the PoE chip.
S/W version	The firmware version of the PoE chip.

15-4 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#
```

16. Reboot Commands

16-1 reboot

This command is used to reboot the Switch.

reboot [force_agree]

Parameters

force_agree	(Optional) Specifies to restart the Switch without confirmation.

Default

None.

Command Mode

Privileged EXEC Mode.

Command Default Level

Level: 15.

Usage Guideline

This command is used to reboot the Switch.

Example

This example shows how to reboot the Switch.

```
Switch# reboot force_agree

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

16-2 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, 2018 at 11pm.

```
Switch# reboot schedule at 23:00 27mar2018
Switch#
```

16-3 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 2018 23:00:00 (in 520 minutes)
 Save before reboot: Yes


Switch#
```

17. Secure Shell (SSH) Commands

17-1 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#
```

17-2 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#
```

17-3 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)#
```

17-4 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)#
```

17-5 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)#
```

17-6 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, 2018-03-15
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#
```

17-7 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#
```

17-8 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/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.

17-9 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***]}**

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.

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)#
```

18. Switch Port Commands

18-1 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)#
```

18-2 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)#
```

19. System File Management Commands

19-1 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)#
```

19-2 boot image

This command is used to specify the file that will be used as the image file for the next boot.

boot image [check] *URL*

Parameters

check	(Optional) Specifies to display the firmware information for the specified file. This information includes the version number and model description.
URL	Specifies the URL of the file to be used as the boot image file.

Default

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: 2.10.012
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)#
```

19-3 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#
```

19-4 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...
```

19-5 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#
```

19-6 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: //192.168.1.123/2.10.012.had flash: image.had

Address of remote host [192.168.1.123]?
Source filename [2.10.012.had]?
Destination filename [image.had]?
 Accessing tftp://192.168.1.123/2.10.012.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#
```

19-7 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#
```

19-8 show running-config

This command is used to display the commands in the running configuration file.

show running-config [effective | all] [interface *INTERFACE-ID***]**

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.

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 2.10.012
!           Copyright(C) 2018 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
```

19-9 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 2.10.012
!           Copyright(C) 2018 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
```

20. System Log Commands

20-1 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#
```

20-2 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)#
```

20-3 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)#
```

20-4 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)#
```

20-5 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)#
```

20-6 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)#
```

20-7 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* **[severity {***SEVERITY-LEVEL* **|** *SEVERITY-NAME***}] [facility {***FACILITY-NUM* **|** *FACILITY-NAME***}] [discriminator** *NAME***] [port** *UDP-PORT***]**

no logging server *IP-ADDRESS*

Parameters

IP-ADDRESS	Specifies the IP address of the SYSLOG server host.
SEVERITY-LEVEL	(Optional) Specifies the severity level of system messages. The messages at that severity level or a more severe level will be logged to message buffers. This value must be between 0 and 7. 0 is the most severe level. The corresponding severity levels are listed together with their respective severity names: emergencies (**0**), alerts (**1**), critical (**2**), errors (**3**), warnings (**4**), notifications (**5**), informational (**6**), debugging (**7**). If 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)#
```

20-8 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     2018-03-15 16:01:58 CRIT(2) System started up
#3     2018-03-15 16:01:58 CRIT(2) System warm start
#2     2018-03-15 15:59:42 CRIT(2) System started up
#1     2018-03-15 15:59:42 CRIT(2) System warm start

Switch#
```

21. Time Commands

21-1 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#
```

21-2 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           : 17:25:47, 2018-03-15
     Time Zone              : UTC +00:00
     Daylight Saving Time   : Disabled

Switch#
```

22. Virtual LAN (VLAN) Commands

22-1 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 port to display the VLAN related setting.
,	(Optional) Specifies a series of interfaces or separates a range of interfaces from a previous range. No space is allowed before or after the comma.
-	(Optional) Specifies a range of interfaces. No space is allowed before or after the hyphen.

Default

None.

Command Mode

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#
```

22-2 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)#
```

22-3 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)#
```

22-4 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)#
```

22-5 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)#
```

22-6 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)#
```

22-7 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)#
```

22-8 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)#
```

22-9 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 2.10.012 Runtime Image ..............  100 %
  UART init ................................................  100 %
```

```
Password Recovery Mode

Switch(reset-config)#
```

In the “Password Recovery Mode” only the following commands can be used.

no enable password	This command is used to delete all account level passwords.
no login password	This command is used to clear the local login methods.
no username	This command is used to delete all local user accounts.
password-recovery	This command is used to initiate the password recovery procedure.
reload	This command is used to save and reboot the Switch.
reload clear running-config	This command is used to reset the running configuration to the factory default settings and then reboot the Switch.
show running-config	This command is used to display the current running configuration.
show username	This command is used to display local user account information.

Appendix B - System Log Entries

The following table lists all possible entries and their corresponding meanings that will appear in the System Log of this Switch.

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.	

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. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event Description: Firmware uploaded unsuccessfully. Log Message: [Unit <unitID>,]Firmware uploaded by <session> unsuccessfully (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address.	Warning

macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	
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. serverIP: Server IP address. pathFile: Path and file name on server.	Informational
Event Description: Configuration uploaded unsuccessfully. Log Message: [Unit <unitID>,]Configuration uploaded by <session> unsuccessfully. (Username: <username>[, IP: <ipaddr>, MAC: <macaddr>], Server IP: <serverIP>, File Name: <pathFile>) Parameters Description: unitID: The unit ID. session: The user's session. username: Represent current login user. ipaddr: Represent client IP address. macaddr: Represent client MAC address. serverIP: Server IP address. pathFile: Path and file name on server.	Warning
Event Description: Unknown type files downloaded unsuccessfully.	Warning

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.	

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

Login/Logout

Log Description	Severity
Event Description: Login through console successfully. Log Message: [Unit <unitID>,]Successful login through Console (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Login through console unsuccessfully. Log Message: [Unit <unitID>,] Login failed through Console (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Warning
Event Description: Console session timed out. Log Message: [Unit <unitID>,] Console session timed out (Username: <username>) Parameters Description: unitID: The unit ID. username: Represent current login user.	Informational
Event Description: Logout through console. Log Message: [Unit <unitID>,] Logout through Console (Username: <username>) Parameters Description: unitID: The unit ID.	Informational

username: Represent current login user.	
Event Description: Login through Telnet successfully. Log Message: Successful login through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through Telnet unsuccessfully. Log Message: Login failed through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Warning
Event Description: Telnet session timed out. Log Message: Telnet session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through Telnet. Log Message: Logout through Telnet (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH successfully. Log Message: Successful login through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Login through SSH unsuccessfully. Log Message: Login failed through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Critical
Event Description: SSH session timed out. Log Message: SSH session timed out (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational
Event Description: Logout through SSH. Log Message: Logout through SSH (Username: <username>, IP: <ipaddr>) Parameters Description: username: Represent current login user. ipaddr: Represent client IP address.	Informational

OpenFlow

Log Description	Severity
Event Description: This log will be generated when the 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 the 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 the flow setting from the controller 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 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

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