D-Link®
Building Networks for People

xStack®

CLI Reference Guide

Product Model: xStack® DGS-3200 Series
Layer 2 Managed Gigabit Ethernet Switch
Release 2.00

IPv6 READY

Table of Contents

I. Introduction

The Introduction section includes the following chapter: Using Command Line Interface.

1 Using Command Line Interface

The Switch can be managed through the Switch's serial port, Telnet, or the Web-based management agent. The Command Line Interface (CLI) can be used to configure and manage the Switch via the serial port or Telnet interfaces.

This manual provides a reference for all of the commands contained in the CLI. Every command will be introduced in terms of purpose, format, description, parameters, and examples. Configuration and management of the Switch via the Web-based management agent are discussed in the User Manual. For detailed information on installing hardware please also refer to the User Manual.

1-1 Accessing the Switch via the Serial Port

The Switch's serial port's default settings are as follows:

- **115200 baud**
- **no parity**
- **8 data bits**
- **1 stop bit**

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above is then connected to the Switch's serial port via an RS-232 DB-9 cable.
With the serial port properly connected to a management computer, the following screen should be visible.

```
                        DGS-3200-10 Gigabit Ethernet Switch
                                Command Line Interface


                               Firmware: Build 2.00.012
                     Copyright(C) 2011 D-Link Corporation. All rights reserved.
UserName:
```

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3200-10:4#**. This is the command line where all commands are input.

1-2 Setting the Switch's IP Address

Each Switch must be assigned its own IP Address, which is used for communication with an SNMP network manager or other TCP/IP application (for example BOOTP, TFTP). The Switch's default IP address is 10.90.90.90. You can change the default Switch IP address to meet the specification of your networking address scheme.

The Switch is also assigned a unique MAC address by the factory. This MAC address cannot be changed, and can be found on the initial boot console screen – shown below.

```
  Boot Procedure                                                    V1.00.016
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100%

  MAC Address    : 00-24-01-15-1C-96
 H/W Version   : B1

  Please Wait, Loading V2.00.012  Runtime Image .............  100%

  Device Discovery .....................................       |
```

The Switch's MAC address can also be found in the Web management program on the Switch Information (Basic Settings) window on the Configuration menu.

The IP address for the Switch must be set before it can be managed with the Web-based manager. The Switch IP address can be automatically set using BOOTP or DHCP protocols, in which case the actual address assigned to the Switch must be known.

The IP address may be set using the Command Line Interface (CLI) over the console serial port as follows:

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, you can enter **config ipif System ipaddress xxx.xxx.xxx.xxx/z**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **z** represents the corresponding number of subnets in CIDR notation.

The IP interface named **System** on the Switch can be assigned an IP address and subnet mask which can then be used to connect a management station to the Switch's Telnet or Web-based management agent

```
DGS-3200-10:4#config ipif System ipaddress 10.24.22.100/255.0.0.0
Command: config ipif System ipaddress 10.24.22.100/8

Success.

DGS-3200-10:4#
```

In the above example, the Switch was assigned an IP address of 10.24.22.100 with a subnet mask of 255.0.0.0. The

system message **Success** indicates that the command was executed successfully. The Switch can now be configured and managed via Telnet, SNMP MIB browser and the CLI or via the Web-based management agent using the above IP address to connect to the Switch

There are a number of helpful features included in the CLI. Entering the **?** command will display a list of all of the top-level commands.

```
..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear address_binding nd_snoop binding_entry ports
clear arptable
clear attack_log
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
clear mld_snooping statistics counter
clear port_security_entry port
clear wac auth_state
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

When entering a command without its required parameters, the CLI will prompt you with a **Next possible completions:** message.

```
DGS-3200-10:4#config account
Command: config account
Next possible completions:
<username 15>

DGS-3200-10:4#
```

In this case, the command **config account** was entered without the parameter **<username>**. The CLI will then prompt to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

In addition, after typing any given command plus one space, users can see all of the next possible sub-commands, in sequential order, by repeatedly pressing the **Tab** key.

To re-enter the previous command at the command prompt, press the up arrow cursor key. The previous command will appear at the command prompt.

```
DGS-3200-10:4#config account
Command: config account
Next possible completions:
<username 15>

DGS-3200-10:4#config account
```

In the above example, the command **config account** was entered without the required parameter **<username>**, the CLI returned the **Next possible completions: <username>** prompt. The up arrow cursor control key was pressed to re-enter the previous command (**config account**) at the command prompt. Now the appropriate username can be entered and the **config account** command re-executed.

All commands in the CLI function in this way. In addition, the syntax of the help prompts are the same as presented in this manual – angle brackets < > indicate a numerical value or character string, braces { } indicate optional parameters or a choice of parameters, and brackets [ ] indicate required parameters.

If a command is entered that is unrecognized by the CLI, the top-level commands will be displayed under the **Available commands:** prompt

```
DGS-3200-10:4#the
Available commands:
..                  ?                   cable_diag          clear
config              create              debug               delete
disable             download            enable              login
logout              no                  ping                ping6
reboot              reconfig            reset               save
show                smtp                telnet              traceroute
upload

DGS-3200-10:4#
```

The top-level commands consist of commands such as **show** or **config**. Most of these commands require one or more parameters to narrow the top-level command. This is equivalent to **show** what? or **config** what? Where the what? is the next parameter.

For example, entering the **show** command with no additional parameters, the CLI will then display all of the possible next parameters.

```
ipv6                ipv6route           jumbo_frame         jwac
l2protocol_tunnel   lacp_port           led
limited_multicast_addr                  link_aggregation    lldp
lldp_med            log                 log_save_timing     loopdetect
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       name_server         nlb
packet              password_recovery   per_queue           port
port_security       ports               power_saving        pppoe
private_vlan        pvid                radius              router_ports
safeguard_engine    scheduling          scheduling_mechanism
serial_port         session             sim                 smtp
snmp                sntp                ssh                 ssl
stp                 switch              syslog              system_severity
tech_support        terminal            tftp                time
time_range          traffic             traffic_segmentation
trusted_host        utilization         vlan                vlan_trunk
voice_vlan          wac

DGS-3200-10:4#
```

In the above example, all of the possible next parameters for the **show** command are displayed. At the next command prompt, the up arrow was used to re-enter the **show** command, followed by the **account** parameter. The CLI then displays the user accounts configured on the Switch.

1-3 Command Syntax Symbols

angle brackets <>	Enclose a variable or value. Specify the variable or value. For example, in the syntax: **show packet ports <portlist>** a port list must be supplied for **<portlist>** when entering the command. Do not type the angle brackets.
square brackets [ ]	Enclose a required value or list of required arguments. One or more values or arguments must be specified. For example, in the syntax: **show utilization [ports | cpu]** either **ports** or **cpu** must be specified when entering the command. Do not type the square brackets.
vertical bar |	Separates mutually exclusive items in a list, one of which must be entered. For example, in the syntax: **config snmp warmstart_traps [enable | disable]** either **enable** or **disable** must be specified when entering the command. Do not type the vertical bar.
braces { }	Enclose an optional value or a list of optional arguments. One or more values or arguments can be specified. For example, in the syntax: **show stp ports {<portlist>}** a range or list of ports can be selected if desired. Otherwise, the switch will simply assume every STP-enabled port should be displayed. Do not type the braces.
ipif <ipif_name 12> **metric <value 1-31>**	12 means the maximum length of IP interface name. 1-31 means the legal range of metric value.

1-4 Line-Editing Keys

Keys	Description
Delete	Delete character under cursor and shift remainder of line to left.
Backspace	Delete character to left of cursor and shift remainder of line to left.
CTRL + R	Toggle on and off. When toggled on, inserts text and shifts previous text to right.
Left Arrow	Move cursor to left.
Right Arrow	Move cursor to right

Tab	Help user to select appropriate token.
P or p	Display the previous page.
N, n or Space	Display the next page.
CTRL+C	Escape from displayed pages.
ESC	Escape from displayed pages.
Q or q	Escape from displayed pages.
R or r	Refresh the displayed pages
A or a	Display the remaining pages. (The screen display will not pause again.)
Enter	Display the next line.

The screen display pauses when the show command output reaches the end of the page.

II. Interface and Hardware

The Interface and Hardware section includes the following chapters: Switch Port, Cable Diagnostics, and File System.

2 Switch Port Command List

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} |10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | [description <desc 1-32> | clear_description]}
show ports {<portlist>} {[description | err_disabled | auto_negotiation | details | media_type]}

2-1 config ports

Purpose

To configure the switch port settings.

Format

config ports [<portlist> | all] {medium_type [fiber | copper]} {speed [auto {capability_advertised {10_half | 10_full | 100_half | 100_full | 1000_full}} |10_half | 10_full | 100_half | 100_full | 1000_full {[master | slave]}] | auto_negotiation [restart_an | remote_fault_advertised [disable | offline | link_fault | auto_negotiation_error]] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | [description <desc 1-32> | clear_description]}

Description

This command is used to change switch port settings.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be configured.
all	To set all ports in the system, use the **all** parameter.
medium_type	Specify the medium type when configuring ports that are combo ports. This is an optional parameter for configuring the medium type of a combo port; If there are no combo ports, a user need not specify **medium_type** in the command.
speed	Set port speed for the specified ports.

	auto	Set port speed to auto negotiation.	
	capability_advertised	Specify that the capability will be advertised.	
		10_half	Set port auto negotiation capability 10_half to be advertised.
		10_full	Set port auto negotiation capability 10_full to be advertised.
		100_half	Set port auto negotiation capability 100_half to be advertised.
		100_full	Set port auto negotiation capability 100_full to be advertised.
		1000_full	Set port auto negotiation capability 1000_full to be advertised.
	10_half	Set port speed to 10_half.	
	10_full	Set port speed to 10_full.	
	100_half	Set port speed to 100_half.	
	100_full	Set port speed to 100_full._	
	1000_full	**1000_full** sets port speed to 1000_full. When setting port speed to **1000_full**, a user should specify master or slave mode for 1000 base TX interface, and leave the **1000_full** without any master or slave setting for other interface.	
	master	Set to master.	
	slave	Set to slave.	
auto_negotiation	**restart_an**	Specify to restart the auto-negotiation process.	

	remote_fault_advertised	Specify that the remote fault advertisement option will be configured. **disable** - Specify to disable remote fault advertisement. **offline** - Specify that a local device may indicate Offline prior to powering off, running transmitter tests, or removing the local device from the active configuration. If it is set and detected offline, it will advertise at the next auto-negotiation. It interacted for 1000Mbps MAUs. **link_fault**- Specify that if set and local device was detected, a Link_Failure condition indicated by the loss of synchronization, will advertise at the next auto-negotiation. It interacted for 1000Mbps MAUs. **auto_negotiation_error** - Specify the resolution which precludes operation between a local device and link partner advertised at the next auto-negotiation. It interacted for 1000Mbps MAUs.
flow_control	Turn on or turn off flow control on one or more ports by setting **flow_control** to enable or disable.	
learning	Turn on or turn off MAC address learning on one or more ports.	
state	Enable or disable the specified port. If the specified ports are in error-disabled status, configuring their **state** to **enable** will recover these ports from a disabled to an enabled state.	
description	Describe the port interface.	
clear_description	Delete the present description of the port interface	

Note: Fiber ports only support 100M_Full and 1000M_Full.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the speed of ports 1 to 3 to be 10 Mbps, with full duplex, learning enabled, state enabled, and flow control enabled:

```
 DGS-3200-10:4# config ports 1-3 speed 10_full state enable learning enable
flow_control enable
 Command: config ports 1-3 speed 10_full state enable learning enable flow_control
```

```
enable

Success.

DGS-3200-10:4#
```

2-2 show ports

Purpose

To display the current configurations of a range of ports.

Format

show ports {<portlist>} {[description | err_disabled | auto_negotiation | details | media_type]}

Description

This command is used to display the current configurations of a range of ports. If no parameter is specified, all ports will be displayed.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.
description	Indicate if port description will be included in the display .
err_disabled	Indicate if ports are disabled by some reasons will be displayed.
auto_negotiation	Specify to display detailed auto-negotiation information.
details	Specify to indicate if port detail information will be included in the display.
media_type	Specify to display the current port media type.

Restrictions

None.

Example

To display the configuration of ports 1 to 4:

```
DGS-3200-10:4#show ports 1-4
Command: show ports 1-4

Port     Port             Settings              Connection           Address
         State      Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
------  --------  ---------------------  ----------------------  ---------
1       Enabled   Auto/Disabled           100M/Full/None          Enabled
```

```
2        Enabled   Auto/Disabled           Link Down                Enabled
3        Enabled   Auto/Disabled           Link Down                Enabled
4        Enabled   Auto/Disabled           Link Down                Enabled

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the description information of ports 1 to 4:

```
DGS-3200-10:4#show ports 1-4 description
Command: show ports 1-4 description

Port     Port           Settings              Connection          Address
         State    Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
------  --------  ---------------------  ----------------------  --------
1        Enabled   Auto/Disabled          100/Full/None            Enabled
         Description:
2        Enabled   Auto/Disabled          Link Down                Enabled
         Description:
3        Enabled   Auto/Disabled          Link Down                Enabled
         Description:
4        Enabled   Auto/Disabled          Link Down                Enabled
         Description:

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

Note: Connection status has the following situations: Link Down, Speed/Duplex/FlowCtrl (link up), and Err-Disabled.

To display port error-disabled information:

```
DGS-3200-10:4#show ports err-disabled
Command: show ports err-disabled

Port    Port      Connection Status      Reason
        State
------  --------  ---------------------  ----------------
1       Enabled   Err-Disabled           Storm control
        Description: port1.
8       Enabled   Err-Disabled           Storm control
        Description: port8.
```

```
DGS-3200-10:4#
```

3 Cable Diagnostics Command List

cable_diag ports [<portlist>| all]

3-1 cable_diag ports

Purpose

To test copper cables. If there is an error on the cable, the type of error can be determined and the position where the error occurred.

Format

cable_diag ports <portlist>

Description

This command is used to test copper cabling. For 10/100Based-TX link speed RJ45 cable, two pairs of cable will be diagnosed. For 1000Base-T link speed RJ45 cable, four pairs of cable will be diagnosed. The type of cable errors can be open, short, or crosstalk. Open means that the cable in the error pair does not have a connection at the specified position, short means that the cables in the error pair has a short problem at the specified position, and crosstalk means that the cable in the error pair has a crosstalk problem at the specified position.

When a port is in link-up status, the test will obtain the distance of the cable. Since the status is link-up, the cable will not have the short or open problem. The test may still detect the crosstalk problem, however. When a port is in link-down status, the link-down may be caused by many factors.

When the port has a normal cable connection, but the remote partner is powered off, the cable diagnosis can still diagnose the health of the cable as if the remote partner is powered on. When the port does not have any cable connection, the result of the test will indicate no cable. The test will detect the type of error and the position where the error occurs.

Note that this test will consume a low number of packets. Since this test is for copper cable, the port with fiber cable will be skipped from the test.

Parameters

Parameters	Description
portlist	Specify a range of ports to be tested.

Restrictions

None.

Example

To test the cable on ports 1 to 4, and 8:

```
DGS-3200-10:4# cable_diag ports 1-4, 8
Command: cable_diag ports 1-4, 8
Perform Cable Diagnostics ...

 Port     Type          Link Status          Test Result       Cable Length(M)
 ---- ------------ ----------------  ---------------------- -------------
  1     1000Base_T     Link Up        OK                              4
  2     1000Base_T     Link Down      No Cable                        -
  3     1000Base_T     Link Down      No Cable                        -
  4     1000Base_T     Link Down      No Cable                        -
  8     1000Base_T     Link Down      No Cable                        -


DGS-3200-10:4#
```

4 File System Command List [DGS-3200-24 Only]

show storage_media_info
md {<drive_id>} <pathname 255>
rd {<drive_id>} <pathname 255>
cd {<pathname 255>}
dir {<drive_id>} {< pathname 255>}
rename {<drive_id>} <pathname 255> < filename 255>
erase { <drive_id>} <pathname 255>
del {<drive_id>} <pathname 255>
move {<drive_id>} <pathname 255> {<drive_id>}<pathname 255>
copy {<drive_id>} < pathname 255> [{<drive_id>}< pathname 255> | image_id <int 1-n> | config_id <int 1-n> | prom]
copy [image_id <int 1-n> | config_id <int 1-n> | prom | log] {<drive_id>} < pathname 255>
format <drive> [fat16 | fat32] {<label_name 8>}

NOTE:

This command set only applies to DGS-3200-24, which has an SD flash card slot at the front of the Switch (DGS-3200-10 and DGS-3200-16 do not support this feature). Users can plug an SD flash card into the SD flash card slot on the DGS-3200-24 to carry out file management and other administrative tasks.

The design of the file system command is based on the following rules: Each storage media on a unit will be mapped to a drive. Therefore, the size of a drive will be the size of the storage media. C: is the default drive that the file system starts with. The storage media of system Flash has higher priority to be mapped to C:

4-1 show storage_media_info

Purpose

To display the storage media's information.

Format

show storage_media_info

Description

This command is used to display information regarding storage media. There can be one or multiple media on the system. The information for media includes drive number and media identification. Please note that for a standalone device, it is not necessary to specify a unit argument.

Parameters

Parameters	Description
drive_id	Specifiy the drive ID. The format of the drive ID is C:

Restrictions

None.

Example

To display storage media information:

```
DGS-3200-24:4# show storage_media_info
Command: show storage_media_info
 Drive   Media_Type   Size     Label           FS_Type
 -------------------------------------------------------
 C:\     SD Card      438MB    TLD3 MICSD       FAT16


DGS-3200-24:4#
```

4-2 md

Purpose

To make a directory.

Format

md {<drive_id>} <pathname 255>

Description

This command is used to create a directory.

Parameters

Parameters	Description
drive_id	Specify the drive ID. The format of the drive ID is C:
pathname	The name of the directory to be created. The path name can be specified as a full path name.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To make a directory:

```
DGS-3200-24:4# md c:\abc
Command: md c:\abc
```

```
Processing......Done.
Success.

DGS-3200-24:4#
```

4-3 rd

Purpose

To remove a directory.

Format

rd {<drive_id>} <pathname 255>

Description

This command is used to remove a directory. If there are files still in the directory, the command will fail and return an error message.

Parameters

Parameters	Description
drive_id	Specify the drive ID. The format of the drive ID is C:
pathname	The name of the directory to be removed. The path name can be specified as a full path name.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To remove a directory:

```
DGS-3200-24:4# rd c:\abc
Command: rd c:\abc

Processing......Done.
Success.

DGS-3200-24:4#
```

4-4 cd

Purpose

To change a directory to another directory or display the current directory path.

Format

cd {<pathname 255>}

Description

This command is used to change the current directory. The current directory is changed under the current drive. If you want to change the working directory to the directory on another drive, then you need to change the current drive to the desired drive, and then change the current directory. The current drive and current directory will be displayed if the **<pathname>** is not specified.

Parameters

Parameters	Description
pathname	Change the current directory to this directory. The path name can be specified as a full path name.

Restrictions

None.

Example

To change a directory to another directory:

```
DGS-3200-24:4# cd
Command: cd


Unit 2 c:\
Success.


DGS-3200-24:4#
```

4-5 dir

Purpose

To list all of the files located in a directory of a drive.

Format

dir {<drive_id>} {<pathname 255>}

Description

This command is used to list all of the files located in a directory of a drive. If a path name is not specified, then all of the files in the specified drive will be displayed. If none of the parameters are specified, the files in the current drive will be displayed.

Parameters

Parameters	Description
drive_id	Specify the drive ID. If not specified, it refers to the current drive.
pathname	Specify a directory name (in path form).

Restrictions

None.

Example

To list all of the files located in a directory of a drive:

```
DGS-3200-24:4# dir C:
Command: dir C:


unit 1 - C:\


2006/05/10 14:00           run.had        229,8112
2006/04/10 14:00           startup.cfg    2,261
2006/03/10 14:00           log.txt        46,384
2006/03/10 14:00  <dir>    log.txt

total files          3
total directories    1

DGS-3200-24:4#
```

4-6 rename

Purpose

To rename a file.

Format

rename {<drive_id>} <pathname 255> <filename 255>

Description

This command is used to rename a file in the file system. The path name specifies the file (in path form) to be renamed and the file name specifies the new file name. The renamed file will stay in the same directory. Please note that the unit argument is not needed for standalone devices.

Parameters

Parameters	Description
drive_id	Specify the drive ID. If not specified, it refers to the current drive.
pathname	Specify file (in path form) to be renamed.
filename	Specify the new name of the file.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To rename a file:

```
DGS-3200-24:4# rename c:\run.had run1.had
Command: rename c:\run.had run1.had
Processing......Done.
Success.

DGS-3200-24:4#
```

4-7 erase, del

Purpose

To remove a file from the system.

Format

erase {<drive_id>} <pathname 255>

del {<drive_id>} <pathname 255>

Description

This command is used to delete a file stored in the file system.

Parameters

Parameters	Description
drive_id	Specify the drive ID. If not specified, it refers to the current drive.
pathname	Specify file (in path form) to be deleted.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To erase a file:

```
DGS-3200-24:4# erase c:\run.had
Command: erase c:\run.had
Processing......Done.
Success.

DGS-3200-24:4#
```

4-8 move

Purpose

To move a file from one location to another location.

Format

move {<drive_id>} <pathname 255> {drive_id} <pathname 255>

Description

This command is used to move a file around the file system. Files in a drive located in a unit can be moved to another drive located in another unit. Note that when a file is moved, it can be specified whether to be renamed at the same time.

Parameters

Parameters	Description
drive_id	Specify the drive ID. If not specified, it refers to the current drive.
pathname	Specify the path, where the file will be moved to.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To move a file:

```
DGS-3200-24:4# move c:\log.txt c:\log1.txt
Command: move c:\log.txt c:\log1.txt
Processing......Done.
Success.

DGS-3200-24:4#
```

4-9 copy

Purpose

To copy a file.

Format

copy {<drive_id>} < pathname 255> [{<drive_id>}< pathname 255> | image_id <int 1-n> | config_id <int 1-n> | prom]

copy [image_id <int 1-n> | config_id <int 1-n> | prom | log] {<drive_id>} < pathname 255>

Description

This command is used to copy a file to another file in the file system. For a project that does not support file system on the Flash, the system file such as runtime image, configuration, prom, and log can still be copied to media or from media that support a file system via this command using the reserved keyword. The keyword here refers to image_id, config_id, prom, or log.

Parameters

Parameters	Description
drive_id	Specify the drive ID. If not specified, it refers to the current drive.
pathname	Specify the file to be copied (in path form).
pathname	Specify the destination where the file will be copied to (in path form).
image_id	Specify the firmware image to be copied.
config_id	Specify the configuration to be copied.
prom	Specify to copy the prom code.
log	Specify to copy the saved log.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To make a copy of a file:

```
DGS-3200-24:4# copy c:\log.txt c:\log1.txt

Command: copy c:\log.txt c:\log1.txt

Processing......Done.

Success.


DGS-3200-24:4#
```

To make a copy of an image ID:

```
DGS-3200-24:4# copy c:\runtime.had image_id 1

Command: copy c:\runtime.had image_id 1

Processing......Done.

Success.


DGS-3200-24:4#
```

4-10 format

Purpose

To format a drive.

Format

format {<drive>} [fat16 | fat32] {<label_name 8>}

Description

This command is used to format a specific drive.

Parameters

Parameters	Description
drive_id	Specify the drive, for example: C:
fat16	Specify the FAT16 file system.
fat32	Specify the FAT32 file system.
label_name8	Specify the label for the drive.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To format media:

```
DGS-3200-24:4# format c:\ FAT16

Command: format c:\ FAT16


Process.....................Done.

Success.


DGS-3200-24:4#
```

5 Gratuitous ARP Command List

enable gratuitous_arp {ipif <ipif_name 12 >} {trap | log}
disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}
config gratuitous_arp learning [enable | disable]
config gratuitous_arp send dup_ip_detected [enable | disable]
config gratuitous_arp send ipif_status_up [enable | disable]
config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0 -65535>
show gratuitous_arp {ipif <ipif_name 12>}

5-1 enable gratuitous_arp

Purpose

To enable the gratuitous ARP trap and log state.

Format

enable gratuitous_arp {ipif <ipif_name 12 >} {trap | log}

Description

This command is used to enable the gratuitous ARP trap and log state. The Switch can trap and log the IP conflict event to inform the administrator.

Parameters

Parameters	Description
<ipif_name12>	Specify the interface name of L3 interface.
trap	Specify trap. The trap is disabled by default.
log	Specify log. The even log is enabled by default.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable gratuitous ARP:

```
DGS-3200-24:4# enable gratuitous_arp ipif System trap log
Command: enable gratuitous_arp ipif System trap log

Success.

DGS-3200-24:4#
```

5-2 disable gratuitous_arp

Purpose

To disable the gratuitous ARP trap and log state.

Format

disable gratuitous_arp {ipif <ipif_name 12>} {trap | log}

Description

This command is used to disable the gratuitous ARP trap and log state.

Parameters

Parameters	Description
<ipif_name12>	Specify the interface name of L3 interface.
trap	Specify trap. The trap is disabled by default.
log	Specify log. The even log is enabled by default.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To disable gratuitous ARP, the trap, and the log state:

```
DGS-3200-24:4# disable gratuitous_arp ipif System trap log
Command: disable gratuitous_arp ipif System trap log

Success.

DGS-3200-24:4#
```

5-3 config gratuitous_arp learning

Purpose

To enable or disable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets.

Format

config gratuitous_arp learning [enable | disable]

Description

This command is used to enable or disable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets.

Parameters

Parameters	Description
enable	Enable learning of ARP entries based on the received gratuitous ARP packets.
disable	Disable learning of ARP entries based on the received gratuitous ARP packets.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable learning of ARP entries in the ARP cache based on the received gratuitous ARP packets:

```
DGS-3200-24:4# config gratuitous_arp learning enable
Command: config gratuitous_arp learning enable

Success.

DGS-3200-24:4#
```

5-4 config gratuitous_arp send dup_ip_detected

Purpose

To enable or disable the sending of gratuitous ARP requests when a duplicate IP address is detected.

Format

config gratuitous_arp send dup_ip_detected [enable | disable]

Description

This command is used to enable or disable the sending of gratuitous ARP requests when a duplicate IP address is detected. By default, the state is disabled. For this command, duplicate IP detected means that the system received an ARP request packet that is sent by an IP address that matches the system's own IP address. In this case, the system knows that somebody out there is using an IP address that conflicts with that of the system. In order to reclaim the correct host of this IP address, the system can send out the gratuitous ARP request packet for this duplicate IP address.

Parameters

Parameters	Description
enable	Enable the sending of gratuitous ARP requests when a duplicate IP is detected.

disable	Disable the sending of gratuitous ARP requests when a duplicate IP is detected.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable the sending of gratuitous ARP requests when a duplicate IP address is detected:

```
DGS-3200-24:4# config gratuitous_arp send dup_ip_detected enable
Command: config gratuitous_arp send dup_ip_detected enable

Success.

DGS-3200-24:4#
```

5-5 config gratuitous_arp send ipif_status_up

Purpose

To enable or disable the sending of gratuitous ARP requests when the IP interface status becomes up.

Format

config gratuitous_arp send ipif_status_up [enable | disable]

Description

This command is used to enable or disable the sending of gratuitous ARP requests when the IP interface status becomes up. This is used to automatically announce the interface's IP address to other nodes. By default, the state is disabled. When the state is enabled and IP interface is linked up, one gratuitous ARP packet will be broadcast.

Parameters

Parameters	Description
enable	Enable the sending of gratuitous ARP requests when the IPIF status becomes up.
disable	Disable the sending of gratuitous ARP requests when the IPIF status becomes up.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To enable the sending of gratuitous ARP requests when the IP interface status becomes up:

```
DGS-3200-24:4#config gratuitous_arp send ipif_status_up enable
```

```
Command: config gratuitous_arp send ipif_status_up enable

Success.

DGS-3200-24:4#
```

5-6 config gratuitous_arp send periodically ipif

Purpose

To configure the interval for the periodical sending of gratuitous ARP request packets.

Format

config gratuitous_arp send periodically ipif <ipif_name 12> interval <value 0 -65535>

Description

This command is used to configure the interval for the periodical sending of gratuitous ARP request packets.

Parameters

Parameters	Description
<ipif_name12>	Specify the interface name of the L3 interface. The maximum length is 12 characters.
<value 0-66635>	Specify the periodically send gratuitous ARP interval time, in seconds.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure the gratuitous ARP interval to 5 for the IPIF System:

```
DGS-3200-24:4# config gratuitous_arp send periodically ipif System interval 5
Command: config gratuitous_arp send periodically ipif System interval 5

Success.

DGS-3200-24:4#
```

5-7 show gratuitous_arp

Purpose

To display gratuitous ARP configuration.

Format

show gratuitous_arp {ipif <ipif_name 12>}

Description

This command is used to display gratuitous ARP configuration.

Parameters

Parameters	Description
<ipif_name12>	Specify the interface name of the L3 interface.

Restrictions

None.

Example

To display the gratuitous ARP log and trap state:

```
DGS-3200-24:4# show gratuitous_arp
Command: show gratuitous_arp

Send on IPIF Status Up        : Disabled
Send on Duplicate IP Detected : Disabled
Gratuitous ARP Learning       : Disabled

IP Interface Name : System
        Gratuitous ARP Trap                     : Disabled
        Gratuitous ARP Log                       : Enabled
        Gratuitous ARP Periodical Send Interval : 0

Total Entries: 1



DGS-3200-24:4#
```

III. Fundamentals

The Fundamentals section includes the following chapters: Basic Management, Utility, and Power Saving.

6 Basic Management Command List

create account [admin | user] <username 15>
enable password encryption
disable password encryption
config account <username 15>{encrypt [plain_text| sha_1] <password>}
show account
delete account <username 15>
show session
show switch
show environment
show serial_port
config serial_port { baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}
enable clipaging
disable clipaging
enable telnet {<tcp_port_number 1-65535>}
disable telnet
enable web {<tcp_port_number 1-65535>}
disable web
save {[config {[config_id <config_id 1-2> | config_name <filename 32> | log | all]}
save {[config {[config_id <config_id 1-2> | config_name <filename 32> | pathname <pathname 255>]} | log {<pathname 255>} | all]} (DGS-3200-24 only)
config cfg_name config_id <value 1-2> config_name <filename 32>
reboot {force_agree}
reset {[config |system]} {force_agree}
login
logout
config terminal { width [default | <value 80-200>] | type [VT100 | VT220 | Xterm]}
show terminal {[width | type]}

6-1 create account

Purpose

To create user accounts.

Format

create account [admin | user] <username 15>

Description

This command creates user accounts. The username is between 1 and 15 characters, the password is between 0 and 15 characters. The number of account (include admin and user) is up to 8.

Parameters

Parameters	Description
admin <username 15>	The name of the admin account.
user <username 15>	The name of the user account.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create the admin-level user “dlink”:

```
DGS-3200-10:4#create account admin dlink
Command: create account admin dlink

Enter a case-sensitive new password:*****
Enter the new password again for confirmation:*****
Success.

DGS-3200-10:4#
```

To create the user-level user “System”:

```
DGS-3200-10:4##create account user System
Command: create account user System

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3200-10:4#
```

6-2 enable password encryption

Purpose

To create user accounts.

Format

enable password encryption

Description

The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form when it is stored in the configuration file. When password encryption is disabled, the password will be in plain text form when it is stored in the configuration file. However, if the created user account directly uses the encrypted password, the password will still be in the encrypted form.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable password encryption

```
DGS-3200-10:4#enable password encryption
Command: enable password encryption

Success.

DGS-3200-10:4#
```

6-3 disable password encryption

Purpose

To create user accounts.

Format

disable password encryption

Description

The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form when it is

stored in the configuration file. When password encryption is disabled, the password will be in plain text form when it is stored in the configuration file. However, if the created user account directly uses the encrypted password, the password will still be in the encrypted form.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable password encryption

```
DGS-3200-10:4#disable password encryption
Command: disable password encryption

Success.

DGS-3200-10:4#
```

6-4 config account

Purpose

To configure user accounts.

Format

config account <username 15>{encrypt [plain_text| sha_1] <password>}

Description

When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password.

If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-I.

Parameters

Parameters	Description
<username 15>	The name of the account. The account must already be defined.
plain_text	Select to specify the password in plain text form.
sha_1	Select to specify the password in the SHA-1 encrypted form.
<password>	The password for the user account. The lengths of a password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0

	character and can have a maximum of 32 characters. For the encrypted form password, the length is fixed to 35 bytes long. The password is case-sensitive.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the user password of “dlink” account :

```
DGS-3200-10:4#config account dlink
Command: config account dlink

Enter a old password:****
Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.

DGS-3200-10:4#
```

To configure the user password of the “administrator” account :

```
DGS-3200-10:4#config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Command: config account administrator encrypt sha_1
*@&cRDtpNCeBiq15KOQsKVyrA0sAiCIZQwq
Success.

DGS-3200-10:4#
```

6-5 show account

Purpose

To display user accounts.

Format

show account

Description

This command is used to display user accounts that have been created.

Parameters

None.

Restrictions

None.

Example

To display the accounts that have been created:

```
DGS-3200-10:4#show account
Command: show account

 Current Accounts:
 Username              Access Level
 ---------------       ------------
 admin                 Admin
 user                  User

 Total Entries : 2

DGS-3200-10:4#
```

6-6 delete account

Purpose

To delete an existing account.

Format

delete account <username 15>

Description

This command is used to delete an existing account.

Parameters

Parameters	Description
<username 15>	The name of the user who will be deleted.

Restrictions

Only Administrator-level users can issue this command. One active admin user must exist.

Example

To delete the user account “System”:

```
DGS-3200-10:4#delete account System
Command: delete account System

Success.

DGS-3200-10:4#
```

6-7 show session

Purpose

To display a list of currently logged-in users.

Format

show session

Description

This command is used to display a list of current users which are logged in to CLI sessions.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display a list of currently logged-in users:

```
DGS-3200-10:4# show session
Command: show session

ID  Live Time     From                          Level  Name
--  ------------  ----------------------------  -----  ---------------
8   23:37:42.270  Serial Port                    4     Anonymous

Total Entries: 1

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

6-8 show switch

Purpose

Used to display the switch information.

Format

show switch

Description

This command is used to display the switch information.

Parameters

None.

Restrictions

None.

Example

To display the switch information:

```
DGS-3200-10:4#show switch
Command: show switch


Device Type        : DGS-3200-10 Gigabit Ethernet Switch
MAC Address        : 00-24-01-15-1C-96
IP Address         : 10.90.90.90 (Manual)
VLAN Name          : default
Subnet Mask        : 255.0.0.0
Default Gateway    : 0.0.0.0
Boot PROM Version : Build 1.00.016
Firmware Version   : Build 2.00.012
Hardware Version   : B1
Serial Number      : P1R2397000010
System Name        :
System Location    :
System Contact     :
Device Uptime      : 0 days, 0 hours, 2 minutes, 25 seconds
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
MLD Snooping       : Disabled
VLAN Trunk         : Disabled
```

```
Telnet             : Enabled (TCP 23)
Web                : Enabled (TCP 80)
SNMP               : Disabled
RMON               : Disabled
Safeguard Engine   : Disabled
SSL Status         : Disabled
SSH Status         : Disabled
802.1x             : Disabled
Jumbo Frame        : Off
CLI Paging         : Enabled
MAC Notification   : Disabled
Port Mirror        : Disabled
SNTP               : Disabled
DHCP Local Relay   : Disabled
Syslog Global State  : Disabled
Single IP Management : Disabled
Dual Image           : Supported
Password Encryption Status : Disabled
DNS Resolver               : Disabled


DGS-3200-10:4#
```

6-9 show environment

Purpose

To display the device internal temperature.

Format

show environment

Description

This command is used to display the device internal temperature and fan status on the DGS-3200-16, in addition to the internal and external power status on the DGS-3200-24. This command is not supported on the DGS-3200-10.

Parameters

None.

Restrictions

Only the DGS-3200-16 and DGS-3200-24 support this command.

Example

To display the switch internal temperature status (DGS-3200-16):

```
DGS-3200-16:4# show environment
Command: show environment

Side Fan                    Temperature
                             (Celsius)
--------                    -------------
   OK                            47

Note: The warning temperature is above 83 degrees.



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

To display the switch internal temperature, fan, and internal and external power status (DGS-3200-24):

```
DGS-3200-24:4# show environment
Command: show environment

Internal Power     External Power         Left Fan         Temperature
                                                           (Celsius)
--------------     --------------         --------         -----------
         Active               Fail                OK                 34

Note: The warning temperature is above 80 degrees.



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

6-10 show serial_port

Purpose

To display the current serial port setting.

Format

show serial_port

Description

This command is used to display the current serial port setting.

Parameters

None.

Restrictions

None.

Example

To display the serial port setting:

```
DGS-3200-10:4#show serial_port
Command: show serial_port

Baud Rate      : 115200
Data Bits      : 8
Parity Bits    : None
Stop Bits      : 1
Auto-Logout    : 10 mins

DGS-3200-10:4#
```

6-11 config serial_port

Purpose

To configure the serial bit rate that will be used to communicate with the management host and the auto logout time for idle connections.

Format

config serial_port { baud_rate[9600|19200|38400|115200] | auto_logout [never|2_minutes|5_minutes|10_minutes|15_minutes] }

Description

This command is used to configure the serial bit rate that will be used to communicate with the management host and the auto logout time for idle connections.

Parameters

Parameters	Description	
baud_rate	The serial bit rate that will be used to communicate with the management host. There are four options: **9600**, **19200**, **38400**, and **115200**. The default baud rate is 115,200.	
auto_logout	The auto logout time out setting:	
	never	Never timeout.

	2_minutes	When you idle over 2 minutes, the device will auto logout.
	5_minutes	When you idle over 5 minutes, the device will auto logout.
	10_minutes	When you idle over 10 minutes, the device will auto logout.
	15_minutes	When you idle over 15 minutes, the device will auto logout.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the baud rate:

```
DGS-3200-10:4# config serial_port baud_rate 9600
Command: config serial_port baud_rate 9600


Success.


DGS-3200-10:4#
```

6-12 enable clipaging

Purpose

To pause the scrolling of the console screen when the show command displays more than one page.

Format

enable clipaging

Description

This command is used to enable pausing of the screen display when show command output reaches the end of the page. The default setting is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable pausing of the screen display when show command output reaches the end of the page:

```
DGS-3200-10:4#enable clipaging
Command: enable clipaging

Success.

DGS-3200-10:4#
```

6-13 disable clipaging

Purpose

To disable pause the scrolling of the console screen when the show command displays more than one page.

Format

disable clipaging

Description

This command is used to disable pausing of the screen display when show command output reaches the end of the page. The default setting is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable pausing of the screen display when show command output reaches the end of the page:

```
DGS-3200-10:4#disable clipaging
Command: disable clipaging

Success.

DGS-3200-10:4#
```

6-14 enable telnet

Purpose

To manage the switch via Telnet-based management software.

Format

enable telnet {<tcp_port_number 1-65535>}

Description

This command is used to enable Telnet and configure the port number.

Parameters

Parameters	Description
tcp_port_number	The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Telnet protocol is 23. By default, Telnet is enabled with TCP port number 23.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable Telnet and configure a port number:

```
DGS-3200-10:4#enable telnet 23
Command: enable telnet 23

Success.

DGS-3200-10:4#
```

6-15 disable telnet

Purpose

To disable Telnet.

Format

disable telnet

Description

This command is used to disable Telnet.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable Telnet:

```
DGS-3200-10:4#disable telnet
Command: disable telnet

Success.

DGS-3200-10:4#
```

6-16 enable web

Purpose

The switch can be managed via HTTP-based management software.

Format

enable web {<tcp_port_number 1-65535>}

Description

This command is used to enable HTTP and configure the port number.

Parameters

Parameters	Description
tcp_port_number	The TCP port number. TCP ports are numbered between 1 and 65535. The “well-known” TCP port for the Web protocol is 80. By default, Web is enabled with TCP port number 80.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable HTTP and configure port number:

```
DGS-3200-10:4#enable web 80
Command: enable web 80

Note: SSL will be disabled if web is enabled.
Success.

DGS-3200-10:4#
```

6-17 disable web

Purpose

To disable HTTP.

Format

disable web

Description

This command is used to disable HTTP.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable HTTP:

```
DGS-3200-10:4#disable web
Command: disable web

Success.

DGS-3200-10:4#
```

6-18 save

Purpose

To save changes in non-volatile RAM.

Format

save {[config {[config_id <config_id 1-2> | config_name <filename 32> log | all] }

save {[config {[config_id <config_id 1-2> | config_name <filename 32> | pathname <pathname 255>]} | log {<pathname 255>} | all]} (DGS-3200-24 only)

Description

The save command saves changes in non-volatile RAM. If no keyword is specified, save changes will go to the currently active configuration file.

Parameters

Parameters	Description
config_id	Specify the configuration identify number of the indicated configuration.
config_name	Specify the configuration name of the indicated configuration.
log	Save log.

all	Save changes to currently active configuration and save log
pathname	Specifies a pathname on the device file system. This parameter is only supported by DGS-3200-24.

Restrictions

Only Administrator-level users can issue this command.

Example

To save changes to non-volatile RAM:

```
DGS-3200-10:4#save
Command: save

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

DGS-3200-10:4#
```

To save configuration 1 to NV-RAM:

```
DGS-3200-10:4#save config config_id 1
Command: save config config_id 1

Saving configuration 1 to NV-RAM..... Done.

DGS-3200-10:4#
```

To save a log to NV-RAM:

```
DGS-3200-10:4#save log
Command: save log

Saving all system logs to NV-RAM..... Done.

DGS-3200-10:4#
```

To save all the configurations and logs to NV-RAM:

```
DGS-3200-10:4#save all
Command: save all

Saving  configuration and logs to NV-RAM..... Done.

DGS-3200-10:4#
```

6-19 config cfg_name

Purpose

To name a configuration file in the system.

Format

config cfg_name config_id <value 1-2> config_name <filename 32>

Description

This command is used to give an alias for a configuration ID, so other configuration commands can use the configuration name after the alias was created.

Parameters

Parameters	Description
config_id	Specify the configuration file ID.
config_name	Specify the configuration file name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To name a configuration file with the configuration ID of "1" to "cfg_1":

```
DGS-3200-24:4# config cfg_name config_id 1 config_name cfg_1.txt
Command: config cfg_name config_id 1 config_name cfg_1.txt

Success.

DGS-3200-24:4#
```

6-20 reboot

Purpose

To restart the switch.

Format

reboot {force_agree}

Description

This command is used to restart the switch.

Parameters

Parameters	Description
force_agree	Specify to immediately execute the reboot command without further confirmation.

Restrictions

Only Administrator-level users can issue this command.

Example

To restart the switch:

```
DGS-3200-10:4#reboot
Command: reboot

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

6-21 reset

Purpose

To reset all switch parameters.

Format

reset {[config |system]} {force_agree}

Description

This command is used to reset all switch parameters to the factory defaults. If no keyword is specified, all parameters will be reset to default settings except IP address, history log, user account, and greeting banner but the switch will neither save nor reboot.

Parameter

Parameters	Description
config	If you specify the **config** keyword , all parameters are reset to default settings. But device will neither save nor reboot.
system	If you specify the **system** keyword, all parameters are reset to default settings. Then the switch will do factory reset, save, and reboot.

force_agree	Specify and the reset command will be executed immediately without further confirmation.

Restrictions

Only Administrator-level users can issue this command.

Example

To reset all the switch parameters except the IP address, history log, user account, and greeting banner:

```
DGS-3200-10:4#reset
Command: reset

Are you sure you want to proceed with system reset
except IP address, log, user account and banner?(y/n) y
Success.

DGS-3200-10:4#
```

To reset the system configuration settings:

```
DGS-3200-10:4#reset config
Command: reset config

Are you sure you want to proceed with system reset?(y/n) y
Success.

DGS-3200-10:4#
```

To reset all system parameters, save, and restart the switch:

```
DGS-3200-10:4#reset system
Command: reset system

Are you sure you want to proceed with system reset?(y/n)
y-(reset all include configuration, save, reboot )
n-(cancel command) y
Reboot & Load Factory Default Configuration...

Saving configurations and logs to NV-RAM..... Done.
Please wait, the switch is rebooting...
```

6-22 login

Purpose

To login to the switch.

Format

login

Description

This command is used to log in to the switch.

Parameter

None.

Restrictions

None.

Example

To login to the switch:

```
DGS-3200-10:4#login
Command: login


UserName:
```

6-23 logout

Purpose

Used to log out of the switch.

Format

logout

Description

This command is used to logout.

Parameter

None.

Restrictions

None.

Example

To logout of the switch:

```
DGS-3200-10:4#logout
Command: logout

**********
* Logout *
**********

                    DGS-3200-10 Gigabit Ethernet Switch
                           Command Line Interface

                           Firmware: Build 2.00.012
            Copyright(C) 2011 D-Link Corporation. All rights reserved.
UserName:
```

6-24 config terminal width

Purpose

To configure the CLI terminal.

Format

config terminal { width [default | <value 80-200>] | type [VT100 | VT220 | Xterm]}

Description

This command is used to configure the CLI terminal.

Parameters

Parameters	Description
width	Specify as the default terminal width, or a terminal width value between 80 and 200 characters. The default value is 80.
type	Specify for the terminal emulator type. The default value is VT_100.

Restrictions

None.

Examples

To configure the CLI terminal:

```
DGS-3200-10:4#config terminal width default type VT100
Command: config terminal width default type VT100

Success.
```

```
DGS-3200-10:4#
```

6-25 show terminal

Purpose

To display the onfiguration of the CLI terminal.

Format

show terminal {[width | type]}

Description

This command is used to display the onfiguration of the CLI terminal.

Parameters

Parameters	Description
width	Specify to display the CLI terminal width.
type	Specify to display the CLI terminal type.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the CLI terminal:

```
DGS-3200-10:4#show terminal
Command: show terminal

Terminal Configuration
Global terminal width    : 80
Current terminal width   : 80

Glocal terminal type     : VT_100
Current terminal type    : VT_100

DGS-3200-10:4#
```

7 Utility Command List

download [firmware_fromTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {image_id <int 1-2>} | cfg_fromTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[config_id <config_id 1-2> | config_name <filename 32> | increment]}]
download [firmware_fromTFTP{ [<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[image_id <int 1-2> | <pathname 255>]} | cfg_fromTFTP{ [<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[config_id <config_id 1-2> | config_name <filename 32> | increment | <pathname 255>]}] (DGS-3200-24 only)
upload [cfg_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[config_id <config_id 1-2> | config_name <filename 32>]} { [include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>} } {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP{ [<ipaddr> | <ipv6addr> | <domain_name255>] <path_filename 64>} | attack_log_toTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>}]
config firmware image_id <1-2> [delete | boot_up]
config firmware <pathname 255> [boot_up] (DGS-3200-24 only)
config configuration [[config_id <value 1-2> | config_name <filename 32>] [boot_up | delete | active]
config configuration [[config_id <value 1-2> | config_name <filename 32>] [boot_up | delete | active]|pathname <pathname 255> [boot_up | active]] (DGS-3200-24 only)
show firmware information
show config [[effective | modified | current_config | config_in_nvram [config_id <config_id 1-2> | config_name <filename 32>]] { [include | exclude| begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | information]
ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99>}
ping6 <ipv6addr> {times <value 1-255>| size <value 1-6000> | timeout <value 1-10>}
traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}
telnet [<ipaddr> | <domain_name 255>] {tcp_port <value 1-65535>}
config tftp {server [<ipaddr> | <domain_name 255>] | firmware_file <path_filename 64> | cfg_file <path_filename 64> | log_file <path_filename 64> | attack_log_file <path_filename 64> | certificate_file <path_filename 64> | key_file <path_filename 64> | tech_support_file <path_filename 64> | debug_error_log_file <path_filename 64> | sim_firmware_file <path_filename 64> | sim_cfg_file <path_filename 64> | sim_log_file <path_filename 64>}

show tftp

Note: The Interface field is used for addresses on the link-local network. It is recommended that the user enter the specific interface for a link-local IPv6 address. The field may be omitted for global IPv6 addresses. For example,

DGS-3200-10:4#upload cfg_toTFTP fe80::20d:88ff:fe11:7b6c%System DGS-3200.cfg

7-1 download

Purpose

To download and install new firmware or a switch configuration file from a TFTP server.

Format

download [firmware_fromTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {image_id <int 1-2>} | cfg_fromTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[config_id <config_id 1-2> | config_name <filename 32> | increment]}]

download [firmware_fromTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[image_id <int 1-2> | <pathname 255>]} | cfg_fromTFTP{ [<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[config_id <config_id 1-2> | config_name <filename 32> | increment | <pathname 255>]}] (DGS-3200-24 only)

Description

This command is used to download a new firmware or a switch configuration file from a TFTP server. The file can be loaded to different section according to the **image_id** or the **config_id**.

Parameters

Parameters	Description
firmware_fromTFTP	Download and install new firmware on the switch from a TFTP server.
cfg_fromTFTP	Download a switch configuration file from a TFTP server.
<ipaddr>	The IP address of the TFTP server.
<ipv6addr>	The IPv6 address of the TFTP server.
<domain_name 255>	Specify the domain name of the TFTP server. This name can be up to 255 characters long.
<path_filename 64>	The DOS path and filename of the firmware or switch configuration file on the TFTP server. The maximum length is 64.
image_id	Specify the image identify number of the indicated firmware. If no keyword is specified, the Switch will download firmware to the

	boot-up image.
config_id	Specify the configuration identify number of the indicated configuration. If no keyword is specified, the Switch will download and make this configuration file active.
<config_name>	Specify the configuration identify name of the indicated configuration.
increment	Allow the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
<pathname 255>	Specify a file on an SD card file system. This is not necessary when a file system is not supported. [DGS-3200-24 only]

Restrictions

Only Administrator-level users can issue this command.

Examples

Download firmware:

```
DGS-3200-10:4#download firmware_fromTFTP 10.90.90.90 c:/dgs3200_Run_1_5_B019.had
Command: download firmware_fromTFTP 10.90.90.90 c:/dgs3200_Run_1_5_B019.had

Connecting to server.................. Done.
Download firmware..................... Done.   Do not power off !!
Please wait, programming flash......... Done.
Success

DGS-3200-10:4#
```

Download firmware for the DGS-3200-24:

```
DGS-3200-24:4#download firmware_fromTFTP 10.90.90.1 dgs3200.had c:\image.had
Command: download firmware_fromTFTP 10.90.90.1 dgs3200.had c:\image.had

Connecting to server.................. Done.
Download firmware..................... Done.   Do not power off !!
Success

DGS-3200-24:4#
```

7-2 upload

Purpose

To upload a configuration file or the switch history log to a TFTP server.

Format

upload [cfg_toTFTP {[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>} {[config_id <config_id 1-2> | config_name <filename 32>]} { [include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>} } {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | log_toTFTP{ [<ipaddr> | <ipv6addr> | <domain_name255>] <path_filename 64>} | attack_log_toTFTP{[<ipaddr> | <ipv6addr> | <domain_name 255>] <path_filename 64>}]

Description

This command is used to upload either the switch's configuration or the switch's history log to a TFTP server.

Parameters

Parameters	Description
cfg_toTFTP	Specify the switch configuration to be uploaded to the TFTP server.
log_toTFTP	Specify the switch history log to be uploaded to the TFTP server.
attack_log_toTFTP	Specify the switch attack log to be uploaded to the TFTP server.
<ipaddr>	The IP address of the TFTP server.
<ipv6addr>	The IPv6 address of the TFTP server.
<domain_name 255>	Enter the domain name of the TFTP server here. This name can be up to 255 characters long.
<path_filename 64>	Specify the location of the switch configuration file or log on the TFTP server. This file will be replaced by the uploaded file from the switch. The maximum length is 64.
config_id	Specify the configuration identify number of the indicated configuration.
config_name	Specify the configuration identify name of the indicated configuration.
include	Specify to include lines that contain the specified filter string.
exclude	Specify to exclude lines that contain the specified filter string.
begin	The first line that contains the specified filter string will be the first line of the output.
<filter_string 80>	Specify a filter string enclosed by the quotation mark symbol. Thus, the filter string itself cannot contain the quotation mark character. The filter string is case sensitive.

Restrictions

Only Administrator-level users can issue this command.

Examples

To upload configuration file to a TFTP server:

```
DGS-3200-10:4#upload cfg_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\cfg config_id 1
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\cfg config_id 1

Connecting to server... Done.
Upload configuration... Done.

DGS-3200-10:4#
```

To upload a system log to a TFTP server:

```
DGS-3200-10:4#upload log_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\log
Command: upload log_toTFTP 10.48.74.121 c:\cfg\DGS-3200-10\log

Connecting to server... Done.
Upload configuration... Done.

DGS-3200-10:4#
```

7-3 config firmware

Purpose

To configure the specific firmware as a boot up image or to delete the specific firmware.

Format

config firmware image_id <1-2> [delete | boot_up]

config firmware <pathname 255> [boot_up] (DGS-3200-24 only)

Description

This command is used to configure firmware as a boot-up image or to delete the firmware.

Parameters

Parameters	Description
image_id <1-2>	Specify the serial number of the indicated firmware.
pathname	Specify a firmware file on an SD card file system. This is not necessary when the file system is not supported. (DGS-3200-24 only)

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a specific firmware:

```
DGS-3200-10:4#config firmware image_id 2 delete
Command: config firmware image_id 2 delete

Are you sure you want to delete firmware image_id 2?(y/n) y
Success.

DGS-3200-10:4#
```

To configure a specific firmware as a boot-up image:

```
DGS-3200-24:4#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DGS-3200-24:4#
```

7-4 config configuration

Purpose

To configure the specific configuration, boot up or active, or to delete it.

Format

config configuration [[config_id <value 1-2> | config_name <filename 32>] [boot_up | delete | active]

config configuration [[config_id <value 1-2> | config_name <filename 32>] [boot_up | delete | active]|pathname <pathname 255> [boot_up | active]] (DGS-3200-24 only)

Description

This command is used to configure the specific configuration, boot up or active, or to delete it.

Parameters

Parameters	Description
config_id <1-2>	Specify the serial number of the indicated configuration.
config_name	Specify the configuration file name which exists.
boot_up	Specify it as a boot up file.

delete	Specify to delete the configuration.
active	Specify to apply the configuration.
pathname	Specify a configuration file on an SD card file system. This is not necessary when the file system is not supported. (DGS-3200-24 only)

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a specific configuration file:

```
DGS-3200-10:4#config configuration config_id 2 delete
Command: config configuration config_id 2 delete

Success.

DGS-3200-10:4#
```

7-5 show firmware information

Purpose

To display firmware information.

Format

show firmware information

Description

This command is used to display firmware information.

Parameters

None

Restrictions

None.

Example

To display firmware information:

```
DGS-3200-24:4# show firmware information
Command: show firmware information

Image ID    : 1(Boot up firmware)
    Version     : 1.50.B012
    Size        : 3713664 Bytes
    Update Time: 2000/01/01 00:57:40
    From        : 10.5.2.5(Console)
    User        : Anonymous



Image ID    : 2
    Version     : (Empty)
    Size        :
    Update Time:
    From        :

DGS-3200-24:4#
```

7-6 show config

Purpose

To display the configuration or configuration information.

Format

show config [[effective | modified | current_config | config_in_nvram [config_id <config_id 1-2> | config_name <filename 32>]] { [include | exclude| begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}} {[include | exclude | begin] <filter_string 80> {<filter_string 80> {<filter_string 80>}}}}} | information]

Description

This command is used to display the configuration or configuration information.

Parameters

Parameters	Description
effective	Specify to display only commands which affect the behavior of the device.
modified	Specify to display only the commands which are not from the 'reset' default setting.

current_config	Specify the current configuration.
config_in_nvram	???
config_id	Specify the configuration file ID.
config_name	Specify the configuration file name which exists.
include	Specify to include lines that contain the specified filter string.
exclude	Specify to exclude lines that contain the specified filter string.
begin	The first line that contains the specified filter string will be the first line of the output.
<filter_string 80>	Specify a filter string enclosed by the quotation mark symbol.
information	Specify to display the detailed information of a specified configuration.

Restrictions

None.

Example

To display configuration information:

```
DGS-3200-10:4#show config information
Command: show config information

Save Configuration Trap       : Disabled
Upload Configuration Trap     : Disabled
Download Configuration Trap   : Disabled

 ID          : 1(Boot up configuration)
 FileName    :
 Version     : 2.00.012
 Size        : 21461 Bytes
 Updata Time: 2000/01/01 00:10:49
 From Server: Local save(Console)
 By User     : Anonymous


 ID          : 2
 FileName    :
 Version     : 2.00.012
 Size        : 21461 Bytes
 Updata Time: 2000/01/01 00:11:04
 From Server: Local save(Console)
 By User     : admin

DGS-3200-10:4#
```

7-7 ping

Purpose

To test the connectivity between network devices.

Format

ping [<ipaddr> | <domain_name 255>] {times <value 1-255> | timeout <sec 1-99>}

Description

This command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm connectivity between the switch and the remote device.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the host.
<domain_name 255>	Specify the domain name of the host. This name can be up to 255 characters long.
times	The number of individual ICMP echo messages to be sent. If no keyword is specified, an infinite number of ICMP echo messages will be sent. The maximum specified value is 255.
timeout	Define the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.

Restrictions

None.

Example

To send ICMP echo message to “10.51.17.1” for 4 times:

```
DGS-3200-10:4#ping 10.51.17.1 times 4
Command: ping 10.51.17.1 times 4

Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms
Reply from 10.51.17.1, time<10ms

Ping Statistics for 10.51.17.1
Packets: Sent =4, Received =4, Lost =0

DGS-3200-10:4#
```

7-8 ping6

Purpose

To diagnose the connectivity between network devices using IPv6.

Format

ping6 <ip6addr> {times <value 1-255> | size <value 1-6000> | timeout <value 1-10>}

Description

This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then “echo” or return the message. This is used to confirm

connectivity between the switch and the remote device.

Parameters

Parameters	Description
ip6addr	Specify the IPv6 address of the host.
times	The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255.
size	Define the size. A value of 1 to 6000 can be specified.
timeout	Define the time-out period while waiting for a response from the remote device. A value of 1 to 10 can be specified.

Restrictions

Only Administrator-level users can issue this command.

Example

To send ICMP echo message to “3FFE:2::D04D:7878:66D:E5BC” for 10 times:

```
DGS-3200-10:4#ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10
Command: ping6 3FFE:2::D04D:7878:66D:E5BC times 10 size 6000 timeout 10

Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Reply from 3FFE:2::D04D:7878:66D:E5BC, bytes=6000 time<10 ms
Ping Statistics for 3FFE:2::D04D:7878:66D:E5BC
Packets: Sent =10, Received =10, Lost =0

DGS-3200-10:4#
```

7-9 traceroute

Purpose

To trace the routed path between the switch and a destination endstation.

Format

traceroute <ipaddr> {ttl <value 1-60>} {port <value 30000-64900>} {timeout <sec 1-65535>} {probe <value 1-9>}

traceroute [<ipaddr> | <domain_name 255>] {ttl <value 1-60> | port <value 30000-64900> | timeout <sec 1-65535> | probe <value 1-9>}

Description

This command is used to trace a route between the switch and a give host on the network.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the destination end station.
<domain_name 255>	Specify the domain name of the destination end station.
ttl	The time to live value of the trace route request. This is the maximum number of routers The traceroute command will cross while seeking the network path between two devices.
port	The port number. Must be above 1024. The value range is from 30000 to 64900.
timeout	Specify the timeout period while waiting for a response from the remote device. A value of 1 to 65535 seconds can be specified. The default is 5 seconds.
probe	The number of probes. The range is from 1 to 9.

Restrictions

Only Administrator-level users can issue this command.

Example

To trace the routed path between the switch and 10.48.74.121:

```
DGS-3200-10:4#traceroute 10.48.74.121 probe 3
Command: traceroute 10.48.74.121 probe 3

1   <10 ms.     10.48.74.121
1   <10 ms.     10.48.74.121
1   <10 ms.     10.48.74.121

DGS-3200-10:4#
```

7-10 telnet

Purpose

To login a host that supports Telnet.

Format

telnet [<ipaddr> | <domain_name 255>] {tcp_port <value 1-65535>}

Description

This command is used to login a host that supports Telnet.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the Telnet server.
<domain_name 255>	Specify the domain name of the telnet server.
tcp_port	Specify the Telnet server port number to be connected to. If not specified, the default port is 23.

Restrictions

Only Administrator-level users can issue this command.

Example

To Telnet to a host, enter the IP address of the switch:

```
DGS-3200-10:4#telnet 10.90.90.90
Command: telnet 10.90.90.90
```

The following screen will appear:

```
                    DGS-3200-10 Gigabit Ethernet Switch
                          Command Line Interface


                         Firmware: Build 2.00.012
          Copyright(C) 2011 D-Link Corporation. All rights reserved.
UserName:
```

Now proceed as if directly connected from a PC via a serial port.

7-11 config tftp

Purpose

To pre-configure TFTP server and file pathname on the TFTP server.

Format

config tftp {server [<ipaddr> | <domain_name 255>] | firmware_file <path_filename 64> | cfg_file <path_filename 64> | log_file <path_filename 64> | attack_log_file <path_filename 64> | certificate_file <path_filename 64> | key_file <path_filename 64> | tech_support_file <path_filename 64> | debug_error_log_file <path_filename 64> | sim_firmware_file <path_filename 64> | sim_cfg_file <path_filename 64> | sim_log_file <path_filename 64>}

Description

This command is used to pre-configure TFTP server and file pathname on the TFTP server.

Parameters

Parameters	Description
server	Specify the IP address or domain name of the TFTP server.
firmware_file	Specify the path name that supports “download/upload firmware_fromTFTP” function.
cfg_file	Specify the path name that supports “download/upload cfg_fromTFTP” function.
log_file	Specify the path name that supports “upload log_toTFTP” function.
attah_log_file	Specify the path name that supports “upload attack_log_toTFTP” function.
certificate_file	Specify the path name that supports “download ssl certificate” function.
key_file	Specify the path name that supports “download key_file” function.
tech_support_file	Specify the path name that supports “upload tech_support_toTFTP” function.
debug_error_log_file	Specify the path name that supports “debug error_log” function.
sim_firmware_file	Specify the path name that supports “download/upload sim_ms firmware_fromTFTP” function.
sim_cfg_file	Specify the path name that supports “downloa/upload sim_ms configuration_fromTFTP” function.
sim_log_file	Specify the path name that supports “upload sim_ms log_toTFTP” function.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure TFTP server:

```
DGS-3200-10:4# config tftp server 10.90.90.1
Command: config tftp server 10.90.90.1

Success.

DGS-3200-10:4#
```

7-12 show tftp

Purpose

To show TFTP settings.

Format

show tftp

Description

This command is used to show the TFTP server and the file path pre-configured by administer.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show TFTP settings, if pre-configure server IPv4 address, firmware_file and log_file only:

```
DGS-3200-10:4# show tftp
Command: show tftp

TFTP Server Settings
IPv4 Address : 10.90.90.1
Domain Name  :

File Type              Path_filename
--------------------   ----------------------
firmware_file          DGS3200.had
```

```
cfg_file
log_file                log_tmp
attack_log_file
certificate_file
key_file
tech_support_file
debug_error_log_file
sim_firmware_file
sim_cfg_file
sim_log_file

DGS-3200-10:4#
```

8 Power Saving Command List

config power_saving mode { length_detection | link_detection | led |port |hibernation} [enable | disable]
show power_saving {length_detection | link_detection | led | port | hibernation}
config power_saving led [[add |delete] time_range <range_name 32> | clear_time_range]
config power_saving port [<portlist>| all] [[add|delete] time_range <range_name 32> | clear_time_range]
config power_saving hibernation [[add | delete] time_range <range_name 32> | clear_time_range]
config led state [enable | disable]
show led

8-1 config power_saving mode

Purpose

To set the power saving state.

Format

config power_saving mode { length_detection | link_detection | led |port |hibernation} [enable | disable]

Description

This command is used to set the power saving state.

For link detection and length detection function, they apply to the ports with copper media. If the power saving link detection state is enabled, the power is saved by following mechanisms:

1. When no links are detected on the port, the port will automatically turn off and will only wake up the second a single link pulse is sent. While the port is turned off, a simple energy-detect circuit will continuously monitor energy on the cable. The moment energy is detected; the port will turn on fully as to the IEEE specification's requirements. The power saving function is performed while no link is detected and it will not affect the port capabilities while the link is up.
2. When a link is detected on the port, for a shorter cable, the power consumption will be reduced by lowering the signal amplitude, since the signal attenuation is proportional to the cable length. The port will adjust the power based on the cable length and still maintain error free applications from both sides of the link. This mechanism is only available using the hardware support cable diagnostics function.

If the power saving state of port is disabled, all power saving schedules of port will not take effect.

If the power saving state of port LED is disabled, all power saving schedules of port LED will not take effect.

If the power saving state of system hibernation is disabled, all power saving schedules of system hibernation will not take effect.

Parameters

Parameters	Description
link_detection	Specify the power saving link detection state.
length_detection	Specify the length detection used.
led	Specify to configure the power saving state of port LED.
port	Specify to configure the power saving state of port.
hibernation	Specify to configure the power saving state of system hibernation.
enable	Specify to enable power saving state.
disable	Specify to disable power saving state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the power saving state of port, hibernation:

```
DGS-3200-10:4#config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.

DGS-3200-10:4#
```

8-2 show power_saving

Purpose

To show power saving information.

Format

show power_saving

show power_saving {length_detection | link_detection | led | port | hibernation}

Description

This command is used to display power saving information.

Parameters

Parameters	Description
length_detection	Specify to display the power saving link detection state.
link_detection	Specify to display the length detection used.

led	Specify to display the power saving state of port LED.
port	Specify to display the power saving state of port.
hibernation	Specify to display the power saving state of system hibernation.

Restrictions

None.

Examples

To display power saving information:

```
DGS-3200-10:4#show power_saving
Command: show power_saving

 Link Detection State: Enabled
 Length Detection State: Enabled

 Power Saving Configuration On System Hibernation
 ----------------------------------------------------
 State: Enabled

 Power Saving Configuration On Port LED
 ----------------------------------------
 State: Disabled

 Power Saving Configuration On Port
 ----------------------------------------
 State: Enabled

DGS-3200-10:4#
```

8-3 config power_saving led

Purpose

To add or delete the power saving schedule on the port LED.

Format

config power_saving led [[add |delete] time_range <range_name 32> | clear_time_range]

Description

This command is used to add or delete the power saving schedule on the LED of all ports. When any schedule is up, all port's LED will be turned off even device's LED working on PoE mode.

Note: The port LED admin state (configured using the command '**config led state**') gets high priority. If the port LED admin state is disabled, all ports' LED will always be turned off. Currently only three time ranges are supported.

Parameters

Parameters	Description
add	Specify to add a time range.
delete	Specify to delete a time range
time_range	Specify the name of the time range.
clear_time_range	Specify to clear all the time range of port LED.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a time range named "range_1" on port LED:

```
DGS-3200-10:4#config power_saving led add time_range range_1
Command:  config power_saving led add time_range range_1

Success.

DGS-3200-10:4#
```

To delete a time range named "range_2" on LED:

```
DGS-3200-10:4#config power_saving led delete time_range range_2
Command:  config power_saving led delete time_range range_2

Success.
DGS-3200-10:4#
```

8-4 config power_saving port

Purpose

To add or delete the power saving schedule on the port.

Format

config power_saving port [<portlist>| all] [[add|delete] time_range <range_name 32> | clear_time_range]

Description

This command is used to add or delete the power saving schedule on the port. When any schedule is up,

the specific port will be shut down (disabled).

Note: The port's admin state has high priority. If the port's admin state is disabled, the specific port will always be shut down (disabled). Currently only three time ranges are supported.

Parameters

Parameters	Description
<portlist>	Specify a range of ports.
all	Specify all ports.
add	Specify to add a time range.
delete	Specify to delete a time range
time_range	Specify the name of the time range.
clear_time_range	Specify to clear all the time range of port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a time range named "range_1" on port 1:

```
DGS-3200-10:4#config power_saving port 1 add time_range range_1
Command:  config  power_saving port 1 add time_range range_1

Success.

DGS-3200-10:4#
```

To delete a time range named "range_2" on port 1:

```
DGS-3200-10:4# config power_saving port 1 delete time_range range_2
Command:  config power_saving port 1 delete time_range range_2

Success.

DGS-3200-10:4#
```

8-5 config power_saving hibernation

Purpose

To add or delete the power saving schedule on system hibernation.

Format

config power_saving hibernation [[add | delete] time_range <range_name 32> | clear_time_range]

Description

This command is used to add or delete the power saving schedule on system hibernation. When the system enters hibernation mode, the Switch changes to a low power state and is idle. It shuts down all the ports, and all network function does not work. Only the console connection will work via the RS232 port.

Parameters

Parameters	Description
add	Specify to add a time range.
delete	Specify to delete a time range
time_range	Specify the name of the time range.
clear_time_range	Specify to clear all the time range of system hibernation.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a time range named “range_1” on system hibernation:

```
DGS-3200-10:4# config power_saving hibernation add time_range range_1
Command: config power_saving hibernation add time_range range_1

Success.

DGS-3200-10:4#
```

To delete a time range named “range_2” on system hibernation:

```
DGS-3200-10:4#config power_saving hibernation delete time_range range_2
Command: config power_saving hibernation delete time_range range_2

Success.

DGS-3200-10:4#
```

8-6 config led state

Purpose

To configure the LED admin state of all ports.

Format

config led state [enable | disable]

Description

This command is used to configure the LED admin state of all ports. When the port LED admin state is disabled, the LEDs of all ports are turned off. If the port LED admin state is enabled, the port LEDs are controlled by the ports' link status.

Parameters

Parameters	Description
enable	Specify to enable the LED admin state of all ports.
disable	Specify to disable the LED admin state of all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the LED admin state:

```
DGS-3200-10:4#config led state disable
Command: config led state disable

Success.

DGS-3200-10:4#
```

8-7 show led

Purpose

To display the setting of all port's LED admin state.

Format

show led

Description

This command is used to display the setting of all port's LED admin state.

Parameters

None.

Restrictions

None.

Examples

To display the setting of all port's LED admin state:

```
DGS-3200-10:4#show led
Command: show led

Port LED state: Enabled

DGS-3200-10:4#
```

9 Configuration Trap Command List

config configuration trap {save [enable | disable] | upload [enable | disable] | download [enable | disable]}

9-1 config configuration trap

Purpose

To configure the trap status of configuration saving completed, configuration uploading completed and configuration downloading completed.

Format

config configuration trap {save [enable | disable] | upload [enable | disable] | download [enable | disable]}

Description

This command is used to configure the trap status of configuration saving completed, configuration uploading completed and configuration downloading completed. When set to enabled, the SNMP Agent will send a trap while the related operation (save/upload/download the configuration) is successfully completed.

Parameters

Parameters	Description
save	When set to enable, the SNMP agent will send trap while successfully save the configuration to NVRAM.
upload	When set to enable, the SNMP agent will send trap while successfully complete uploading configuration.
download	When set to enable, the SNMP agent will send trap while successfully complete downloading configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the trap of a configuration saving completed:

```
DGS-3200-24:4# config configuration trap save enable

Command:  config configuration trap save enable


Success.


DGS-3200-24:4#
```

10 SD Card Management Command List [DGS-3200-24 Only]

create backup [config | log] time_range <range_name 32> filename<pathname> {state [enable | disable]}
config backup [config | log] time_range <range_name 32> filename <pathname> state [enable | disable]
delete backup [config | log] [all | time_range <range_name 32> {filename <pathname>}]
show backup {config | log}
create execute_config time_range <range_name 32> config <pathname> {state [enable | disable] | [increment | reset]}
config execute_config time_range <range_name 32> config <pathname> {state [enable | disable] | [increment | reset]}
delete execute_config [all | time_range <range_name 32> {config <pathname>}]
show execute_config
execute config <pathname> {increment}

NOTE:

This command set only applies to DGS-3200-24, which has an SD flash card slot at the front of the Switch (DGS-3200-10 and DGS-3200-16 do not support this feature). Users can plug an SD flash card into the SD flash card slot on the DGS-3200-24 to carry out file management and other administrative tasks.

The design of the file system command is based on the following rules: Each storage media on a unit will be mapped to a drive. Therefore, the size of a drive will be the size of the storage media. C: is the default drive that the file system starts with. The storage media of system Flash has higher priority to be mapped to C:

10-1 create backup

Purpose

To create a schedule to backup the configuration or log.

Format

create backup [config | log] time_range <range_name 32> filename<pathname> {state [enable | disable]}

Description

This command is used to create a schedule to backup the configuration or log to file system.
If the time range does not exist, the schedule will still be created without prompt. But the schedule will not take effective until the time range is created. To create an existed entry, the device will feedback a success message and does no change for the existed schedule. The maximum of schedules backup is 15.

Parameters

Parameters	Description
config	Schedule to back up configuration.
log	Schedule to back up log.
time_range	The schedule to back up the configuration or log.
filename	The backup filename of the configuration or log.
state	Enable or disable the backup schedule when the schedule is created. If not specified, the schedule will be disabled.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a backup schedule on time range "range_1":

```
DGS-3200-24:4# create backup config time_range range_1 filename bk-config-1
Command: create backup config time_range range_1 filename bk-config-1

Success.

DGS-3200-24:4#
```

10-2 config backup

Purpose

To enable or disable a schedule backup.

Format

config backup [config | log] time_range <range_name 32> filename <pathname> state [enable | disable]

Description

This command is used to enable or disable a schedule backup.

Parameters

Parameters	Description
config	Schedule to back up configuration.
log	Schedule to back up log.
time_range	The schedule to back up the configuration or log.
filename	The backup filename of the configuration or log.
state	Enable or disable the backup schedule.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable a backup schedule on time range "range_1":

```
DGS-3200-24:4# config backup log time_range range_1 filename bk-des-log state enable
Command: config backup log time_range range_1 filename bk-des-log state enable

Success.

DGS-3200-24:4#
```

10-3 delete backup

Purpose

To delete schedule backup.

Format

delete backup [config | log] [all | time_range <range_name 32> {filename <pathname>}]

Description

This command is used to delete schedule backup.

Parameters

Parameters	Description
config	Schedule to back up configuration.
log	Schedule to back up log.
all	Delete all the schedules.
time_range	The time range of schedule backup that wants to be deleted.
filename	The backup filename of the configuration or log that wants to be deleted.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To delete all the schedules:

```
DGS-3200-24:4# delete backup config all

Command: delete backup config all


Success.


DGS-3200-24:4#
```

10-4 show backup

Purpose

This command is used to show schedule backup.

Format

show backup {config | log}

Description

This command is used to show schedule backup.

Parameters

Parameters	Description
config	Display the backup schedules for configuration.
log	Display the backup schedules for log.

Restrictions

None.

Example

To show all backup schedules:

```
DGS-3200-24:4# show backup
Command: show backup

Backup Schedule Entry 1
Time Range : range_1
Type       : log
Filename   : log-1
State      :  Enabled

Backup Schedule Entry 2
Time Range : range_2
Type       : configuration
Filename   : config-1
State      : Disabled

Total Entries：2

DGS-3200-24:4#
```

10-5 create execute_config

Purpose

To create a schedule to execute the configuration on file system.

Format

create execute_config time_range <range_name 32> config <pathname> {state [enable | disable] | [increment | reset]}

Description

This command is used to create a schedule to execute the configuration on file system. If the time range does not exist, the schedule will still be created without prompt. But the schedule will not take effective until the time range is created. To create an existed entry, the device will feedback a success message and does no change for the existed schedule. The maximum of schedules execute is 15.

Parameters

Parameters	Description
time_range	The time range when the configuration will be executed.

config	The filename of the configuration on file system.
state	Enable or disable the executive schedules when the schedule is created. If not specified, the schedule will be disabled.
increment	The current configuration will not be reset before executing the configuration.
reset	The current configuration will be reset before executing the configuration.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To create a schedule to execute the configuration on file system:

```
DGS-3200-24:4# create execute_config time_range range-1 config vlan-config state enable increment
Command: create execute_config time_range range-1 config vlan-config state enable increment

Success.

DGS-3200-24:4#
```

10-6 config execute_config

Purpose

To configure a executive schedule.

Format

config execute_config time_range <range_name 32> config <pathname> {state [enable | disable] | [increment | reset]}

Description

This command is used to configure configuration state or execute method of a executive schedule.

Parameters

Parameters	Description
time_range	The time range for schedule to execute the configuration.
config	The filename of the configuration on file system.
state	Enable or disable the executive schedules.
increment	If this option is specified, the current configuration will not be reset before executing the configuration.
reset	If this option is specified, the current configuration will be reset before executing the configuration.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To configure a executive schedule:

```
DGS-3200-24:4 config execute_config time_range range_1 config system-config state enable increment
Command: config execute_config time_range range_1 config system-config state enable increment

Success.

DGS-3200-24:4#
```

10-7 delete execute_config

Purpose

To delete the schedule of executing configuration.

Format

delete execute_config [all | time_range <range_name 32> {config <pathname>}]

Description

This command is used to delete the schedule of executing configuration.

Parameters

Parameters	Description
all	Delete all the schedules of executing configuration.
time_range	The time range of the schedules that execute configuration to be deleted.
config	The configuration file name on file system.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To delete all the schedule of executing configuration:

```
DGS-3200-24:4# delete execute_config all
Command: delete execute_config all

Success.

DGS-3200-24:4#
```

10-8 show execute_config

Purpose

To display all the executive schedules.

Format

show execute_config

Description

This command is used t o display all the executive schedules.

Parameters

None.

Restrictions

None.

Example

To display all the executive schedules:

```
DGS-3200-24:4# show execute_config
Command: show execute_config

Execute Schedule entry 1
Time Range  : execute_1
filename   : configuration_1
Method     : Increment
State      : Enabled

Execute Schedule entry 2
Time Range  : execute_2
Filename   : configuration_2
Method     : Reset
State      : Disabled

Total Entries: 2

DGS-3200-24:4#
```

10-9 execute config

Purpose

To execute configuration on file system.

Format

execute config <pathname> {increment}

Description

This command is used to execute configuration on file system.

Parameters

Parameters	Description
<pathname>	The configuration filename on file system.
increment	If not specified, the current configuration will be reset before executing the configuration. If specified, the current configuration will not be reset before executing the configuration.

Restrictions

Only Administrator and Operator-level users can issue this command.

Example

To load and execute a configuration:

```
DGS-3200-24:4# execute config config-vlan-0
Command: execute config config-vlan-0

Read configuration config-vlan-0 failure.

DGS-3200-24:4#
```

11 Password Recovery Command List

enable password_recovery
disable password_recovery
show password_recovery

11-1 enable password_recovery

Purpose

To enable the password recovery mode.

Format

enable password_recovery

Description

This command is used to enable the password recovery mode.

Note: The configuration does not take effect until being saved.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the password recovery mode:

```
DGS-3200-10:4# enable password_recovery
Command: enable password_recovery


Success.


DGS-3200-10:4#
```

11-2 disable password_recovery

Purpose

To disable the password recovery mode.

Format

disable password_recovery

Description

This command is used to disable the password recovery mode.

Note: The configuration does not take effect until being saved.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the password recovery mode:

```
DGS-3200-10:4# disable password_recovery
Command: disable password_recovery

Success.

DGS-3200-10:4#
```

11-3 show password_recovery

Purpose

To display the password recovery state.

Format

show password_recovery

Description

The command is used to display the password recovery state. The displayed content includes both the running configuration and the NV-RAM configuration.

When the password recovery state is enabled a user can reboot the switch and enter into the Password Recovery mode. Otherwise, if the Password Recovery state is disabled a user will not be able to enter into the special recovery mode.

Note: Only the NV-RAM configuration will take effect when the switch restarts next time, the running configuration does not take effect until saved. That means the password recovery is determined by the state stored in the NV-RAM and take effect at the next time switch start up. The Running Configuration is the current configured state of the password recovery, it will lost without save, or become the NV-RAM configuration if save the configurations.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the password recovery state:

```
DGS-3200-10:4# show password_recovery
Command: show password_recovery

 Running Configuration   : Disabled
 NV-RAM Configuration    : Enabled

DGS-3200-10:4#
```

12 Tech Support Command List

show tech_support
upload tech_support_toTFTP {<ipaddr> <path_filename 64>}

12-1 show tech_support

Purpose

To display technical support information.

Format

show tech_support

Description

This command is used to display technical support information. It is especially useful for technical support personnel that need to view the overall device operation information.

Parameters

None

Restrictions

Only Administrator-level users can issue this command.

Examples

To display technical support information:

```
DGS-3200-10:4# show tech_support
Command: show tech_support


#------------------------------------------------------------------------------
#                 DGS-3200-10 Gigabit Ethernet Switch
#                    Technical Support Information
#
#                      Firmware: Build 2.00.006
#        Copyright(C) 2011  D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------


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


[SYS 2000-1-1 00:53:38]
```

```
Boot Time         : 1 Jan 2000  00:00:00
RTC Time          : 2000/1/1 00:53:38
Boot PROM Version   : Build 1.00.016
Firmware Version    : Build 2.00.006
Hardware Version    : B1
Serial number      : P1R2397000010
MAC Address        : 00-24-01-15-1C-96
[ERROR_LOG 2000-1-1 00:53:38]

 Error log is empty.

********************  System Log  ********************

[SYS_LOG 2000-1-1 00:53:38]

Index Date      Time    Log Text

----- ---------- -------- ---------------------------------------------------

DGS-3200-10:4#
```

12-2 upload tech_support_toTFTP

Purpose

To upload technical support information to a TFTP server.

Format

upload tech_support_toTFTP {<ipaddr> <path_filename 64>}

Description

This command is used to upload technical support information to a TFTP server. This command can be interrupted by Ctrl – C or ESC when it is executing.

Parameters

Parameters	Description
<ipaddr>	Specify the IPv4 address of the TFTP server.
<path_filename 64>	Specify the file name of the technical support information file sent to the TFTP server. The maximum size of the file name is 64 characters.

Restrictions

Only Administrator-level users can issue this command.

Examples

To upload technical support information:

```
DGS-3200-10:4# upload tech_support_toTFTP 10.0.0.66 tech_suppport.txt
Command: upload tech_support_toTFTP 10.0.0.66 tech_suppport.txt

Connecting to server.................. Done.
Upload techsupport file.............. Done.

Success.

DGS-3200-10:4#
```

IV. Network Management

The Fundamentals section includes the following chapters: SNMPv1/v2, SNMPv3, Network Management, Network Monitoring, System Severity, Command List History, Modify Banner and Prompt, Time and SNTP, Jumbo Frame, Single IP Management, and Safeguard Engine.

13 SNMPv1/v2 Command List

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community <community_string 32>
show snmp community <community_string 32>

Note: If SNMPv3 commands are used, the SNMPv1/v2 commands are not necessary.

13-1 create snmp community

Purpose

To create an SNMP community string.

Format

create snmp community <community_string 32> view <view_name 32> [read_only | read_write]

Description

This command is used to create an SNMP community string and to specify the string as enabling read only or read-write privileges for the SNMP management host.

Parameters

Parameters	Description
community_string	An alphanumeric string of up to 32 characters used in the authentication of users wanting access to the switch's SNMP agent.
view	An alphanumeric string of up to 32 characters.
read_only	Allow the above community string user to have read-only access to the switch's SNMP agent. The default read-only community string is public.
read_write	Allow the above community string user to have read and write access to the switch's SNMP agent. The default read-write community string is private.

Restrictions

Only Administrator-level users can issue this command. A maximum of four community strings can be specified.

Example

To create a read-only level SNMP community "System":

```
DGS-3200-10:4# create snmp community System view CommunityView read_write
Command: create snmp community System view CommunityView read_write

Success.

DGS-3200-10:4#
```

13-2 delete snmp community

Purpose

To delete an SNMP community string previously entered on the switch.

Format

delete snmp community <community_string 32>

Description

This command is used to delete an SNMP community string entered on the switch using the create snmp community command above.

Parameters

Parameters	Description
community_string	An alphanumeric string of up to 32 characters used in the authentication of users wanting access to the switch's SNMP agent.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a read-only level SNMP community "System":

```
DGS-3200-10:4#delete snmp community System
Command: delete snmp community System

Success.

DGS-3200-10:4#
```

13-3 show snmp community

Purpose

To display the SNMP community configurations on the switch.

Format

show snmp community <community_string 32>

Description

This command is used to display the following information: SNMP community strings, View Name, and Access Rights.

Parameter

Parameters	Description
community_string	An alphanumeric string of up to 32 characters used in the authentication of users wanting access to the switch's SNMP agent.

Restrictions

None.

Example

To display SNMP community information:

```
DGS-3200-10:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                          View Name                   Access Right
---------------------------------  ---------------------- -----------
Private                                 CommunityView               read_write
Public                                  CommunityView               read_only

Total Entries: 2

DGS-3200-10:4#
```

14 SNMPv3 Command List

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20 >] priv [none | des <priv_password 8-16>]| by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none | des) <priv_key 32-32>]]}
delete snmp user <user_name 32>
show snmp user
show snmp groups
create snmp view <view_name 32> <oid> view_type [included | excluded]
delete snmp view <view_name 32> [all | <oid>]
show snmp view {<view_name 32>}
create snmp community <community_string 32> view <view_name 32> [read_only|read_write]
delete snmp community <community_string 32>
show snmp community { <community_string 32> }
config snmp engineID <snmp_engineID 10-64>
show snmp engineID
create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}
delete snmp group <groupname 32>
create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>
delete snmp [host <ipaddr> | v6host <ipv6addr>]
show snmp v6host { <ipv6addr> }
show snmp host { <ipaddr> }
show snmp traps

Note: If SNMPv3 commands are used, SNMPv1/v2 commands are not necessary.

14-1 create snmp user

Purpose

To create a new user to an SNMP group originated by this command.

Format

create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20 >] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32>| sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}

Description

This command is used to create a new user to an SNMP group originated by this command. Users can choose to input authentication and privacy by using a password or key.

Parameters

Parameters	Description	
user_name	The name of the user on the host that connects to the agent. The range is 1 to 32 .	
groupname	The name of the group to which the user is associated. The range is 1 to 32 .	
encrypted	Specify whether the password appears in encrypted format.	
by_password	indicate input password for authentication and privacy	
by_key	Indicate an input key for authentication and privacy	
auth	Indicate an authentication level setting session. The options are MD5 and SHA .	
	md5	The HMAC-MD5-96 authentication level.
	sha	The HMAC-SHA-96 authentication level.
auth_password	An authentication string used by MD5 or SHA1.	
priv_password	A privacy string used by DES.	
auth_key	An authentication key used by MD5 or SHA1. It is a hex string type.	
priv_key	A privacy key used by DES. It is a hex string type.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a new user to an SNMP group originated by this command:

```
DGS-3200-10:4#create snmp user dlink D-Link_group encrypted by_password auth md5
12345678 priv des 12345678
Command: create snmp user dlink D-Link_group encrypted by_password auth md5 1234
5678 priv des 12345678

Success.

DGS-3200-10:4#
```

14-2 delete snmp user

Purpose

To remove a user from an SNMP group and delete the associated group in SNMP group.

Format

delete snmp user <user_name 32>

Description

This command is used to remove a user from an SNMP group and deletes the associated group in the SNMP group.

Parameters

Parameters	Description
username	The name of the user on the host that connects to the agent. The range is 1 to 32 .

Restrictions

Only Administrator-level users can issue this command.

Example

To delete an SNMP user:

```
DGS-3200-10:4#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3200-10:4#
```

14-3 show snmp user

Purpose

To display information on each SNMP username in the group username table.

Format

show snmp user

Description

This command is used to display information on each SNMP username in the group username table.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display SNMP user information:

```
DGS-3200-10:4#show snmp user
Command: show snmp user

Username                         Group Name                       VerAuthPriv
-------------------------      -------------------------         -----------
initial                          initial                          V3 NoneNone

Total Entries : 1

DGS-3200-10:4#
```

14-4 show snmp groups

Purpose

To display the names of groups on the switch, and the security model, level, and the status of the different views.

Format

show snmp groups

Description

This command is used to display the names of groups on the switch, and the security model, level, and the status of the different views.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the names of the SNMP groups on the switch:

```
DGS-3200-10:4#show snmp groups
Command: show snmp groups

Vacm Access Table Settings

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : public
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Group    Name    : initial
ReadView Name    : restricted
WriteView Name   :
Notify View Name : restricted
Security Model   : SNMPv3
Security Level   : NoAuthNoPriv

Group    Name    : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : private
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv2
```

```
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : ReadGroup
ReadView Name    : CommunityView
WriteView Name   :
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv1
Security Level   : NoAuthNoPriv

Group    Name    : WriteGroup
```

```
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv2
Security Level   : NoAuthNoPriv

Group    Name    : D-Link_group
ReadView Name    : CommunityView
WriteView Name   : CommunityView
Notify View Name : CommunityView
Security Model   : SNMPv3
Security Level   : authPriv

Total Entries: 10

DGS-3200-10:4
```

14-5 create snmp view

Purpose

To assign views to community strings to limit which MIB objects an SNMP manager can access.

Format

create snmp view <view_name 32> <oid> view_type [included | excluded]

Description

This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.

Parameters

Parameters	Description	
view_name	View name to be created.	
oid	Object-Identified tree, MIB tree.	
view_type	Specify the access type of the MIB tree in this view.	
	included	Includes this view.
	excluded	Excludes this view.

Restrictions

Only Administrator-level users can issue this command.

Example

To assign views to community strings to limit which MIB objects an SNMP manager can access:

```
DGS-3200-10:4#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3200-10:4#
```

14-6 delete snmp view

Purpose

To remove a view record.

Format

delete snmp view <view_name 32> [all | <oid>]

Description

This command is used to remove a view record.

Parameters

Parameters	Description
<view_name 32>	View name of the user who will be deleted.
all	All view records.
oid	Object-Identified tree, MIB tree.

Restrictions

Only Administrator-level users can issue this command.

Example

To remove a view record:

```
DGS-3200-10:4#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3200-10:4#
```

14-7 show snmp view

Purpose

To display SNMP view records.

Format

show snmp view {<view_name 32>}

Description

This command is used to display SNMP view records.

Parameters

Parameters	Description
<view_name 32>	View name of the user who likes to show.

Restrictions

Only Administrator-level users can issue this command.

Example

To display SNMP view records:

```
DGS-3200-10:4#show snmp view
Command: show snmp view

Vacm View Table Settings
View Name              Subtree                      View Type
--------------------  -------------------------  ----------
restricted             1.3.6.1.2.1.1               Included
restricted             1.3.6.1.2.1.11              Included
restricted             1.3.6.1.6.3.10.2.1          Included
restricted             1.3.6.1.6.3.11.2.1          Included
restricted             1.3.6.1.6.3.15.1.1          Included
CommunityView          1                            Included
CommunityView          1.3.6.1.6.3                 Excluded
CommunityView          1.3.6.1.6.3.1               Included

Total Entries: 8

DGS-3200-10:4#
```

14-8 create snmp community

Purpose

Use an SNMP community string to define the relationship between the SNMP manager and the agent. The community string acts like a password to permit access to the agent on the switch. You can specify one or more of the following characteristics associated with the string:

An access list of IP addresses of the SNMP managers that are permitted to use the community string to gain access to the agent.

A MIB view, which defines the subset of all MIB objects accessible to the given community.
Read and write or read-only permission for the MIB objects accessible to the community.

Format

create snmp community <community_string 32> view <view_name 32> [read_only|read_write]

Description

This command is used to create an SNMP community string.

Parameters

Parameters	Description
<community_string 32>	Community string. Max string length is 32.
view_name	View name. A MIB view. Max length is 32
read_only	Read-only permission.
read_write	Read and write permission.

Restrictions

Only Administrator-level users can issue this command.

Example

To create an SNMP community string:

```
DGS-3200-10:4#create snmp community dlink view CommunityView read_write
Command: create snmp community dlink view CommunityView read_write

Success.

DGS-3200-10:4#
```

14-9 delete snmp community

Purpose

To remove a specific community string

Format

delete snmp community <community_string 32>

Description

This command is used to remove a specific community string.

Parameters

Parameters	Description
<community_string 32>	The community string that will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete an SNMP community:

```
DGS-3200-10:4#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3200-10:4#
```

14-10 show snmp community

Purpose

To display community string configurations

Format

show snmp community { <community_string 32> }

Description

This command is used to display community string configurations. If a community string is not specified, all community string information will be displayed.

Parameters

Parameters	Description
<community_string 32>	The community string to be displayed.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the current community string configurations:

```
DGS-3200-10:4#show snmp community
Command: show snmp community

SNMP Community Table
Community Name                 View Name                     Access Right
---------------------------  ---------------------------  ------------
private                        CommunityView                 read_write
public                         CommunityView                 read_only

Total Entries : 2

DGS-3200-10:4#
```

14-11 config snmp engineID

Purpose

To configure an identifier for the SNMP engine on the switch.

Format

config snmp engineID <snmp_engineID 10-64>

Description

This command is used to configure an identifier for the SNMP engine on the switch. Associated with each SNMP entity is a unique engineID.

Parameters

Parameters	Description
<snmp_engineID 10-64>	Identify for the SNMP engine on the switch. It is an octet string type.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure an identifier for the SNMP engine on the switch:

```
DGS-3200-10:4#config snmp engineID 1023457890
Command: config snmp engineID 1023457890

Success.

DGS-3200-10:4#
```

14-12 show snmp engineID

Purpose

To display the identification of the SNMP engine on the switch.

Format

show snmp engineID

Description

This command is used to display the identification of the SNMP engine on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the identification of an SNMP engine:

```
DGS-3200-10:4#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 1023457890

DGS-3200-10:4#
```

14-13 create snmp group

Purpose

To create a new SNMP group, or a table that maps SNMP users to SNMP views

Format

create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}

Description

This command is used to create a new SNMP group.

Parameters

Parameters	Description	
groupname	The name of the group.	
v1	The least secure of the possible security models.	
v2c	The second least secure of the possible security models.	
v3	The most secure of the possible security models. Specifies authentication of a packet.	
	noauth_nopriv	neither support packet authentication nor encrypting.
	auth_nopriv	Support packet authentication .
	auth_priv	Support packet authentication and encrypting.
view_name	View name. A MIB view.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a new SNMP group:

```
DGS-3200-10:4#create snmp group D-Link_group v3 auth_priv read_view CommunityView
write_view CommunityView notify_view CommunityView
Command: create snmp group D-Link_group v3 auth_priv read_view CommunityView wri
te_view CommunityView notify_view CommunityView

Success.

DGS-3200-10:4#
```

14-14 delete snmp group

Purpose

To remove an SNMP group.

Format

delete snmp group <groupname 32>

Description

This command is used to remove an SNMP group.

Parameters

Parameters	Description
groupname	The name of the group will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To remove an SNMP group:

```
DGS-3200-10:4#delete snmp group D_Link_group
Command: delete snmp group D_Link_group

Success.

DGS-3200-10:4#
```

14-15 create snmp host

Purpose

To create a recipient of an SNMP trap operation.

Format

create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

Description

This command is used to create a recipient of an SNMP operation.

Parameters

Parameters	Description
ipaddr	The IP address of the recipient for which the traps are targeted.
v6host	Specify the v6host IP address to which the trap packet will be sent.
v1	The least secure of the possible security models.
v2c	The second least secure of the possible security models.
v3	The most secure of the possible.

	noauth_nopriv	neither support packet authentication nor encrypting.
	auth_nopriv	Support packet authentication .
	auth_priv	Support packet authentication and encrypting.
auth_string	The authentication string.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a recipient of an SNMP operation:

```
DGS-3200-10:4#create snmp host 10.48.74.100 v3 noauth_nopriv initial
Command: create snmp host 10.48.74.100 v3 noauth_nopriv initial

Success.

DGS-3200-10:4#
```

14-16 delete snmp host

Purpose

To delete a recipient of an SNMP trap operation.

Format

delete snmp [host <ipaddr> | v6host <ipv6addr>]

Description

This command is used to delete a recipient of an SNMP trap operation.

Parameters

Parameters	Description
ipaddr	The IP address of the recipient for which the traps are targeted.
v6host	Specify the v6host IP address.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a recipient of an SNMP trap operation:

```
DGS-3200-10:4#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100
```

```
Success.

DGS-3200-10:4#
```

14-17 show snmp host

Purpose

To display the recipient for which the traps are targeted.

Format

show snmp host {<ipaddr>}

Description

This command is used to display the recipient for which the traps are targeted. If no parameter specified, all SNMP hosts will be displayed.

Parameters

Parameters	Description
<ipaddr>	The IP address of the recipient for which the traps are targeted.

Restrictions

None.

Example

To display the recipient for which the traps are targeted:

```
DGS-3200-10:4# show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version     Community Name / SNMPv3 User Name
---------------  ---------------  ---------------------------------
10.48.76.100     V3 noauthnopriv  initial
10.51.17.1       V2c               public

Total Entries : 2

DGS-3200-10:4#
```

14-18 show snmp v6host

Purpose

To display the recipient for which the traps are targeted.

Format

show snmp v6host { <ipv6addr> }

Description

This command is used to display the recipient for which the traps are targeted. If no parameters are specified, all SNMP hosts will be displayed.

Parameters

Parameters	Description
<ipv6addr>	Specify the v6host IP address.

Restrictions

None.

Example

To display the recipient for which the traps are targeted:

```
DGS-3200-10:4# show snmp v6host
Command: show snmp v6host

SNMP Host Table
-----------------------------------------------------------------
Host IPv6 Address: FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF
SNMP Version     : V3 na/np
Community Name/SNMPv3 User Name: 12345678910234567890

Host IPv6 Address: FECO:1A49:2AA:FF:FE34:CA8F
SNMP Version     : V3 a/np
Community Name/SNMPv3 User Name: abcdefghijk

Total Entries : 2

DGS-3200-10:4#
```

14-19 show snmp traps

Purpose

To display the status of SNMP trap and authentication traps.

Format

show snmp traps

Description

This command is used to show the trap state.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the SNMP trap and authentication trap status:

```
DGS-3200-10:4#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Trap   : Enabled
Linkchange Traps    : Enabled
Coldstart Traps     : Enabled
Warmstart Traps     : Enabled

DGS-3200-10:4#
```

15 Network Management Command List

enable snmp
disable snmp
create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}
config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] [{snmp | telnet | ssh | http | https | ping} | all]
delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]
show trusted_host
config snmp system_name {<sw_name>}
config snmp system_location {<sw_location>}
config snmp system_contact {<sw_contact>}
enable rmon
disable rmon
enable snmp traps
disable snmp traps
enable snmp authenticate_traps
disable snmp authenticate_traps
enable snmp linkchange_traps
disable snmp linkchange_traps
config snmp coldstart_traps [enable | disable]
config snmp warmstart_traps [enable | disable]
config snmp linkchange_traps ports [all | <portlist>] [enable | disable]
show snmp traps {linkchange_traps {ports <portlist>} }

15-1 enable snmp

Purpose

To enable the SNMP interface access function.

Format

enable snmp

Description

This command is used to enable the SNMP function. When SNMP function is disabled, the network

manager will not be able the access SNMP MIB objects. The device will not send traps or notification to network manager either.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP:

```
DGS-3200-10:4#enable snmp
Command: enable snmp

Success.

DGS-3200-10:4#
```

15-2 disable snmp

Purpose

To disable the SNMP interface access function.

Format

disable snmp

Description

This command is used to disable the SNMP function. When SNMP function is disabled, the network manager will not be able the access SNMP MIB objects. The device will not send traps or notification to network manager either.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNMP:

```
DGS-3200-10:4#disable snmp
Command: disable snmp

Success.

DGS-3200-10:4#
```

15-3 create trusted_host

Purpose

To create the trusted host.

Format

create trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] {snmp | telnet | ssh | http | https | ping}

Description

This command is used to create the trusted host. The switch allows you to specify up to thirty IP addresses that are allowed to manage the switch via in-band SNMP or Telnet based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the switch, provided the user knows the Username and Password.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the trusted host.
<ipv6addr>	Specify the IPv6 address of the trusted host.
network	Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.
ipv6_prefix	Specify the IPv6 network address of the trusted network.
snmp	Specify the trusted host for SNMP.
telnet	Specify the trusted host for Telnet.
ssh	Specify the trusted host for SSH.
http	Specify the trusted host for HTTP.
https	Specify the trusted host for HTTPS.
ping	Specify the trusted host for Ping.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a trusted host:

```
DGS-3200-10:4#create trusted_host 10.48.74.121
Command: create trusted_host 10.48.74.121

Success.

DGS-3200-10:4#
```

15-4 config trusted_host

Purpose

To configure the access interfaces for the trusted host.

Format

config trusted_host [<ipaddr> | <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr>] [add | delete] [{snmp | telnet | ssh | http | https | ping} | all]

Description

This command is used to configure the access interfaces for the trusted host.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the trusted host.
<ipv6addr>	Specify the IPv6 address of the trusted host.
network	Specify the network address of the trusted network. The form of network address is xxx.xxx.xxx.xxx/y.
ipv6_prefix	Specify the IPv6 network address of the trusted network.
add	Allow to manage applications for a trusted host.
delete	Prevent from managing applications for a trusted host.
snmp	Specify the trusted host for SNMP.
telnet	Specify the trusted host for Telnet.
ssh	Specify the trusted host for SSH.
http	Specify the trusted host for HTTP.
https	Specify the trusted host for HTTPs.
ping	Specify the trusted host for Ping.
all	Specify the trusted host for all applications.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the trusted host:

```
DGS-3200-10:4# config trusted_host 10.48.74.121 add ssh telnet
Command: config trusted_host 10.48.74.121 add ssh telnet

Success.

DGS-3200-10:4#
```

15-5 delete trusted_host

Purpose

To delete a trusted host entry made using the **create trusted_host** command above.

Format

delete trusted_host [ipaddr <ipaddr> | ipv6address <ipv6addr> | network <network_address> | ipv6_prefix <ipv6networkaddr> | all]

Description

This command is used to delete a trusted host entry made using the **create trusted_host** command above.

Parameters

Parameters	Description
ipaddr	The IP address of the trusted host
ipv6address	Specify the IPv6 address of the trusted host.
network	The network address of the trusted network.
ipv6_prefix	Specify the IPv6 network address of the trusted network.
all	Specify **all** to delete all trusted host entries.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete the trusted host with an IP address of 10.48.74.121:

```
DGS-3200-10:4#delete trusted_host ipaddr 10.48.74.121
Command: delete trusted_host ipaddr 10.48.74.121

Success.

DGS-3200-10:4#
```

15-6 show trusted_host

Purpose

To display a list of trusted hosts entered on the switch using the **create trusted_host** command above.

Format

show trusted_host

Description

This command is used to display the trusted hosts.

Parameters

None.

Restrictions

None.

Example

To display a trusted host:

```
DGS-3200-10:4#show trusted_host
Command: show trusted_host



Management Stations

IP Address                                      Access Interface
-----------------------------------------------------------------
10.48.74.121                                    SNMP Telnet SSH HTTP HTTPs Ping

Total Entries: 1



DGS-3200-10:4#
```

15-7 config snmp system_name

Purpose

To configure the name for the switch.

Format

config snmp system_name {<sw_name>}

Description

This command is used to configure the name of the switch.

Parameter

Parameters	Description
sw_name	A maximum of 255 characters is allowed. A null string is also accepted.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the switch name for “DGS-3200-10 Gigabit Ethernet Switch”:

```
DGS-3200-10:4# config snmp system_name DGS-3200-10 Gigabit Ethernet Switch
Command: config snmp system_name DGS-3200-10 Gigabit Ethernet Switch


Success.
```

```
DGS-3200-10:4#
```

15-8 config snmp system_location

Purpose

To enter a description of the location of the switch.

Format

config snmp system_location {<sw_location>}

Description

This command is used to enter a description of the location of the switch. A maximum of 255 characters can be used.

Parameter

Parameters	Description
sw_location	A maximum of 255 characters is allowed. A null string is also accepted.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the switch location for “HQ 5F”:

```
DGS-3200-10:4# config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3200-10:4#
```

15-9 config snmp system_contact

Purpose

To enter the name of a contact person who is responsible for the switch.

Format

config snmp system_contact {<sw_contact>}

Description

This command is used to enter the name and/or other information to identify a contact person who is

responsible for the switch. A maximum of 255 characters can be used.

Parameters

Parameters	Description
sw_contact	A maximum of 255 characters is allowed. A null string is also accepted.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the switch contact to “MIS Department IV”:

```
DGS-3200-10:4#config snmp system_contact "MIS Department IV"
Command: config snmp system_contact "MIS Department IV"

Success.

DGS-3200-10:4#
```

15-10 enable rmon

Purpose

To enable RMON on the switch.

Format

enable rmon

Description

This command is used to enable RMON on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable RMON on the switch:

```
DGS-3200-10:4#enable rmon
Command: enable rmon
```

```
Success.

DGS-3200-10:4#
```

15-11 disable rmon

Purpose

To disable RMON on the switch.

Format

disable rmon

Description

This command is used to disable RMON on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable RMON on the switch:

```
DGS-3200-10:4#disable rmon
Command: disable rmon

Success.

DGS-3200-10:4#
```

15-12 enable snmp traps

Purpose

To enable SNMP trap support.

Format

enable snmp traps

Description

This command is used to enable SNMP trap support on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP trap support:

```
DGS-3200-10:4#enable snmp traps
Command: enable snmp traps

Success.

DGS-3200-10:4#
```

15-13 disable snmp traps

Purpose

To disable SNMP trap support on the switch.

Format

disable snmp traps

Description

This command is used to disable SNMP trap support on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To prevent SNMP traps from being sent from the switch:

```
DGS-3200-10:4#disable snmp traps
Command: disable snmp traps

Success.

DGS-3200-10:4#
```

15-14 enable snmp authenticate_traps

Purpose

To enable SNMP authentication failure trap support.

Format

enable snmp authenticate_traps

Description

This command is used to enable SNMP authentication failure trap support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP authentication trap support:

```
DGS-3200-10:4#enable snmp authenticate_traps
Command: enable snmp authenticate_traps


Success.


DGS-3200-10:4#
```

15-15 disable snmp authenticate_traps

Purpose

To disable SNMP authentication failure trap support.

Format

disable snmp authenticate_traps

Description

This command is used to disable SNMP authentication failure trap support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNMP authentication trap support:

```
DGS-3200-10:4#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3200-10:4#
```

15-16 enable snmp linkchange_traps

Purpose

To configure the sending of linkchange traps.

Format

enable snmp linkchange_traps

Description

This command is used to enable SNMP linkchange traps.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNMP linkchange traps:

```
DGS-3200-10:4#enable snmp linkchange_traps
Command: enable snmp linkchange_traps

Success.

DGS-3200-10:4#
```

15-17 disable snmp linkchange_traps

Purpose

To disable SNMP linkchange traps.

Format

disable snmp linkchange_traps

Description

This command is used to disable SNMP linkchange traps.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNMP linkchange traps:

```
DGS-3200-10:4#disable snmp linkchange_traps
Command: disable snmp linkchange_traps

Success.

DGS-3200-10:4#
```

15-18 config snmp coldstart_traps

Purpose

To configure a trap for a coldstart event.

Format

config snmp coldstart_traps [enable | disable]

Description

This command is used to configure the trap state for a coldstart event.

Parameters

Parameters	Description
enable	Enable a trap of a coldstart event. The default state is enabled.
disable	Disable a trap of a coldstart event.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the trap state for a coldstart event:

```
DGS-3200-10:4#config snmp coldstart_traps enable
Command: config snmp coldstart_traps enable

Success.

DGS-3200-10:4#
```

15-19 config snmp warmstart_traps

Purpose

To configure the trap state for a warmstart event.

Format

config snmp warmstart_traps [enable | disable]

Description

This command is used to configure the trap state for a warmstart event.

Parameters

Parameters	Description
enable	Enable a trap of a warmstart event. The default state is enabled.
disable	Disable a trap of a warmstart event.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the trap state for a warmstart event:

```
DGS-3200-10:4#config snmp warmstart_traps enable
Command: config snmp warmstart_traps enable

Success.

DGS-3200-10:4#
```

15-20 config snmp linkchange_traps ports

Purpose

To configure the sending of linkchange traps and per port control for the sending of change traps.

Format

config snmp linkchange_traps ports [all] <portlist>] [enable | disable]

Description

This command is used to configure the sending of linkchange traps and per port control for the sending of change traps.

Parameters

Parameters	Description
all	Specify all ports.
<portlist>	Specify a port range.
enable	Enable sending a linkchange trap for this port.
disable	Disable sending a linkchange trap for this port.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the sending of linkchange traps and per port control for the sending of change traps:

```
DGS-3200-10:4#config snmp linkchange_traps ports 1-4 enable
Command: config snmp linkchange_traps ports 1-4 enable

Success.

DGS-3200-10:4#
```

15-21 show snmp traps

Purpose

To display the status of SNMP traps and authentication traps.

Format

show snmp traps

Description

This command is used to display trap states.

Parameters

Parameters	Description
linkchange_traps	Specify to include linkchange traps on this list.

ports	Specify to include ports on this list.
<portlist>	To specify a port range.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the status of SNMP traps and authentication traps:

```
DGS-3200-10:4#show snmp traps
Command: show snmp traps

SNMP Traps          : Enabled
Authenticate Trap   : Enabled
Linkchange Traps    : Enabled
Coldstart Traps     : Enabled
Warmstart Traps     : Enabled

DGS-3200-10:4#
```

To display the status of linkchange traps:

```
DGS-3200-10:4#show snmp traps linkchange_traps
Command: show snmp traps linkchange_traps

Linkchange Traps    : Enabled

  Port 1 : Enabled
  Port 2 : Enabled
  Port 3 : Enabled
  Port 4 : Enabled
  Port 5 : Enabled
  Port 6 : Enabled
  Port 7 : Enabled
  Port 8 : Enabled
  Port 9 : Enabled
  Port 10: Enabled

DGS-3200-10:4#
```

16 Network Monitoring Command List

show packet ports <portlist>
show error ports <portlist>
show utilization [ports | cpu]
show utilization dram
show utilization flash
clear counters {ports <portlist> }
clear log
show log {index <value_list> }
enable syslog
disable syslog
show syslog
config syslog host [all|<index 1-4>] { severity [informational |warning |all] | **facility [local0|local1|local2|local3|local4|local5|local6|local7] |** **udp_port <udp_port_numer> |** **ipaddress <ipaddr> |** **state [enable|disable]}**
create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational|warning|all] | **facility[local0|local1|local2|local3|local4|local5|local6|local7] |udp_port <udp_port_number> | state** **[enable|disable]}**
delete syslog host [<index 1-4> | all]
show syslog host {<index 1-4>}
config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]
show log_save_timing

16-1 show packet ports

Purpose

To display statistics about the packets sent and received by the switch.

Format

show packet ports <portlist>

Description

This command is used to display statistics about the packets sent and received by the switch.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Example

To display the packets analysis for port 7:

```
DGS-3200-10:4#show packet ports 7
Command: show packet ports 7

Port number : 7
================================================================================
Frame Size/Type  Frame Counts           Frames/sec
---------------  --------------------   --------------------
64               572                    27
65-127           151                    5
128-255          39                     0
256-511          65                     0
512-1023         7                      0
1024-1518        0                      0
Unicast RX       4                      0
Multicast RX     162                    1
Broadcast RX     568                    31

Frame Type       Total                  Total/sec
----------       --------------------   --------------------
RX Bytes         81207                  2237
RX Frames        734                    32
TX Bytes         8432                   0
TX Frames        100                    0
DGS-3200-10
```

16-2 show error ports

Purpose

To display the error statistics for a range of ports.

Format

show errors ports <portlist>

Description

This command is used to display error statistics for a range of ports.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Example

To display the errors of port 3:

```
DGS-3200-10:4#show error ports 3
Command: show error ports 3

Port number : 3
               RX Frames                              TX Frames
               ---------                              ---------
CRC Error       0                     Excessive Deferral    0
Undersize       0                     CRC Error             0
Oversize        0                     Late Collision        0
Fragment        0                     Excessive Collision   0
Jabber          0                     Single Collision      0
Drop Pkts       0                     Collision             0
Symbol Error    0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

16-3 show utilization

Purpose

To display real-time port or CPU utilization statistics.

Format

show utilization [ports | cpu]

Description

This command is used to display real-time port or CPU utilization statistics.

Parameters

None.

Restrictions

None.

Example

To display port utilization:

```
DGS-3200-10:4# show utilization ports
Command: show utilization ports

Port    TX/sec       RX/sec       Util
------  ----------   ----------   ----
1      0            0            0
2      0            0            0
3      0            0            0
4      0            0            0
5      0            0            0
6      0            0            0
7      0            0            0
8          0                   0                    0
```

To display CPU utilization:

```
DGS-3200-10:4# show utilization cpu
Command: show utilization cpu

CPU utilization :
-------------------------------------------------------------------------------
Five seconds - 20%        One minute - 10%         Five minutes - 70%


CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

16-4 show utilization dram

Purpose

To display real-time DRAM utilization statistics.

Format

show utilization dram

Description

This command is used to display real-time DRAM utilization statistics.

Parameters

None.

Restrictions

None.

Examples

To display DRAM utilization:

```
DGS-3200-10:4#show utilization dram
Command: show utilization dram

DRAM utilization :
        Total DRAM    : 131072  KB
        Used DRAM     :  116519  KB
        Utilization   :  88%



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

16-5 show utilization flash

Purpose

To display real-time Flash utilization statistics.

Format

show utilization flash

Description

This command is used to display real-time Flash utilization statistics.

Parameters

None.

Restrictions

None.

Examples

To display Flash utilization:

```
DGS-3200-10:4# show utilization flash
Command: show utilization flash

FLASH Memory Utilization :
        Total FLASH    : 16384   KB
        Used FLASH     :  7798   KB
        Utilization    :  47%

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

16-6 clear counters

Purpose

To clear the switch's statistics counters.

Format

clear counters {ports <portlist>}

Description

This command is used to clear the switch's statistics counters. If no parameter is specified, the system will count all of the ports.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured. The beginning and end of the port list range are separated by a dash.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear the switch's statistics counters for ports 7 to 9:

```
DGS-3200-10:4#clear counters ports 7-9
Command: clear counters ports 7-9

Success.
```

```
DGS-3200-10:4#
```

16-7 clear log

Purpose

To clear the switch's history log.

Format

clear log

Description

This command is used to clear the switch's history log.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the switch's history log:

```
DGS-3200-10:4#clear log
Command: clear log

Success

DGS-3200-10:4#
```

16-8 show log

Purpose

To display the switch history log.

Format

show log {index <value_list> }

Description

This command is used to display the switch history log. If no parameter is specified, all history log entries will be displayed.

Parameters

Parameters	Description
value_list	Display the history log between two values. For example, **show log index 1-5** will display the history log from 1 to 5.

Restrictions

None.

Examples

To display the switch history log:

```
DGS-3200-10:4#show log index 1-5
Command: show log index 1-5

Index  Date      Time        Log Text
-----  ------------------  --------------------------------------------------
5      2000-01-01 00:00:41  Port 5 link down
4      2000-01-01 00:00:31  Port 3 link up, 100Mbps FULL duplex
3      2000-01-01 00:00:31  Successful login through Console (Username:Anonymous)
2      2000-01-01 00:00:31  Console session timed out (Username: dlink)
1      2000-01-01 00:00:31  Spanning Tree Protocol is disabled

DGS-3200-10:4#
```

16-9 enable syslog

Purpose

To enable syslog to send a message.

Format

enable syslog

Description

This command is used to enable syslog to send a message.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable syslog to send a message:

```
DGS-3200-10:4#enable syslog
Command: enable syslog


Success
DGS-3200-10:4#
```

16-10 disable syslog

Purpose

To disable syslog from sending a message.

Format

disable syslog

Description

This command is used to disable syslog from sending a message.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable syslog sending a message:

```
DGS-3200-10:4#disable syslog
Command: disable syslog


Success


DGS-3200-10:4#
```

16-11 show syslog

Purpose

To display the syslog protocol global state.

Format

show syslog

Description

This command is used to display the syslog protocol global state.

Parameters

None.

Restrictions

None.

Examples

To display the syslog protocol global state:

```
DGS-3200-10:4#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3200-10:4#
```

16-12 config syslog host

Purpose

To configure the syslog host configuration.

Format

config syslog host [all |<index 1-4>] { severity [informational |warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable |disable]}

Description

This command is used to configure the syslog host configuration

Parameters

Parameters	Description	
all	Specify all hosts.	
<index 1-4>	Specify the host index.	
severity	Three levels of support:	
	informational	informational messages
	warning	warning conditions
	all	any condition

facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now.	
	local0	user-defined Facility
	local1	user-defined Facility
	local2	user-defined Facility
	local3	user-defined Facility
	local4	user-defined Facility
	local5	user-defined Facility
	local6	user-defined Facility
	local7	user-defined Facility
udp_port	The UDP port number.	
ipaddr	The IP address of the host.	
state	The syslog protocol has been used for the transmission of event notification messages across networks to host. This option enables or disables the host to receive such messages.	

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the syslog host configuration:

```
DGS-3200-10:4#config syslog host all severity all facility local0
Command: config syslog host all severity all facility local0

Success.

DGS-3200-10:4#
```

16-13 create syslog host

Purpose

To add a new syslog host.

Format

create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational|warning|all] |

facility[local0|local1|local2|local3|local4|local5|local6|local7] |udp_port <udp_port_number> | state [enable|disable]}

Description

This command is used to add a new syslog host.

Parameters

Parameters	Description	
<index 1-4>	The host index.	
severity	Three levels are supported:	
	informational	Informational messages.
	warning	Warning conditions.
	all	Any condition.
facility	Some of the operating system daemons and processes have been assigned Facility values. Processes and daemons that have not been explicitly assigned a Facility may use any of the "local use" facilities or they may use the "user-level" Facility. Those Facilities that have been designated are shown in the following: Bold font means the facility values the switch supports now.	
	local0	user-defined Facility
	local1	user-defined Facility
	local2	user-defined Facility
	local3	user-defined Facility
	local4	user-defined Facility
	local5	user-defined Facility
	local6	user-defined Facility
	local7	user-defined Facility
udp_port	The UDP port number.	
ipaddr	The IP address of the host.	
state	The syslog protocol has been used for the transmission of event notification messages across networks to host. The option enables or disables the host to receive such messages.	

Restrictions

Only Administrator-level users can issue this command.

Example

To create a new syslog host:

```
DGS-3200-10:4#create syslog host 1 severity all facility local0
Command: create syslog host 1 severity all facility local0

Success.

DGS-3200-10:4#
```

16-14 delete syslog host

Purpose

To delete syslog host(s).

Format

delete syslog host [<index 1-4> | all]

Description

This command is used to delete syslog host(s).

Parameters

Parameters	Description
<index 1-4>	Specify the host index.
all	Specify all hosts.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a syslog host:

```
DGS-3200-10:4#delete syslog host 4
Command: delete syslog host 4

Success

DGS-3200-10:4#
```

16-15 show syslog host

Purpose

To display syslog host configurations.

Format

show syslog host {<index 1-4>}

Description

This command is used to display syslog host configurations. If no parameter is specified, all hosts will be displayed.

Parameters

Parameters	Description
index	The host index.

Restrictions

None.

Example

To display syslog host configurations:

```
DGS-3200-10:4#show syslog host
Command: show syslog host

Syslog Global State: Disabled

Host Id  Host IP Address  Severity         Facility  UDP port  Status
-------  ---------------  --------------   --------  --------  --------
1        10.1.1.2         All              Local0    514       Disabled
2        10.40.2.3        All              Local0    514       Disabled
3        10.21.13.1       All              Local0    514       Disabled

Total Entries : 3

DGS-3200-10:4#
```

16-16 config log_save_timing

Purpose

To configure the method to save log.

Format

config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]

Description

This command is used to set the method to save log.

Parameters

Parameters	Description
time_interval	Save log to flash every xxx minutes. (if no log happen in this

	period, don't save)
on_demand	Save log to flash whenever a user types **save log** or **save all**.
log_trigger	Save log to flash whenever log arrives.

Restrictions

Only Administrator-level users can issue this command.

Notes

The default method is **on_demand**.

Examples

To configure method to save log as on demand:

```
DGS-3200-10:4# config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3200-10:4#
```

16-17 show log_save_timing

Purpose

To show the method to save log.

Format

show log_save_timing

Description

This command is used to display the method to save log.

Parameters

None.

Restrictions

None.

Example

To show the timing method of the log save:

```
DGS-3200-10:4#show log_save_timing
Command: show log_save_timing

Saving log method: on_demand
```

```
DGS-3200-10:4#
```

17 System Severity Command List

config system_severity [trap | log | all] [critical | warning | information]
show system_severity

17-1 config system_severity

Purpose

To configure severity level control for the system.

Format

config system_severity [trap | log | all] [critical | warning | information]

Description

This command is used to configure severity level control for the system.

Parameters

Parameters	Description
trap	Configure severity level control for a trap.
log	Configure severity level control for a log.
all	Configure severity level control for a trap and a log.
critical	Severity level = critical.
warning	Severity level = warning.
information	Severity level = information.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure severity level control for information level for a trap:

```
DGS-3200-10:4#config system_severity trap information
Command: config system_severity trap information

Success.

DGS-3200-10:4#
```

17-2 show system_severity

Purpose

To show the severity level control for a system.

Format

show system_severity

Description

This command is used to show the severity level control for a system.

Parameters

None.

Restrictions

None.

Examples

To show the severity level control for a system:

```
DGS-3200-10:4#show system_severity
Command: show system_severity

System Severity Trap : warning
System Severity Log  : information

DGS-3200-10:4#
```

18 Command List History Command List

?
show command_history
config command_history <value 1-40>

18-1 ?

Purpose

To display all the commands in the Command Line Interface (CLI) or specific syntax and description information for an individual command.

Format

? {command}

Description

This command is used to display all of the commands available through the Command Line Interface (CLI) or to specific syntax and description information for an individual command. If no command is specified, the system will display all commands.

Parameters

Parameters	Description
command	Specify the command to display.

Restrictions

None.

Example

To display all commands:

```
DGS-3200-10:4#?
Command: ?


..
?
cable_diag ports
clear
clear address_binding dhcp_snoop binding_entry ports
clear address_binding nd_snoop binding_entry ports
clear arptable
```

```
clear attack_log
clear counters
clear dhcp binding
clear dhcp conflict_ip
clear ethernet_oam ports
clear fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear jwac auth_state
clear log
clear mac_based_access_control auth_state
clear mld_snooping data_driven_group
clear mld_snooping statistics counter
clear port_security_entry port
clear wac auth_state
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

18-2 show command_history

Purpose

To display the command history.

Format

show command_history

Description

This command is used to display the command history.

Parameters

None.

Restrictions

None.

Example

To display the command history:

```
DGS-3200-10:4# show command_history
Command: show command_history

?
?
show traffic_segmentation 1-6
config traffic_segmentation 1-6 forward_list 7-8
config radius delete 1
config radius add 1 10.48.74.121 key dlink default
config 802.1x reauth port_based ports all
config 802.1x init port_based ports all
config 802.1x auth_parameter ports 1-50 direction both
config 802.1x capability ports 1-5 authenticator
show 802.1x auth_configuration ports 1
show 802.1x auth_state ports 1-5
enable 802.1x
show 802.1x auth_state ports 1-5
show igmp_snooping
enable igmp_snooping

DGS-3200-10:4#
```

18-3 config command_history

Purpose

The switch “remembers” the last 40 (maximum) commands you entered. This command lets you configure the number of commands that the switch can recall.

Format

config command_history <value 1-40>

Description

This command is used to configure the number of commands that the switch can recall.

Parameters

Parameters	Description
value	The number of commands (1-40) that the switch can recall.

Restrictions

None.

Example

To configure the number of commands the switch can recall to the last 20 commands:

```
DGS-3200-10:4#config command_history 20
Command: config command_history 20

Success.

DGS-3200-10:4#
```

19 Command Logging Command List

enable command logging
disable command logging
show command logging

19-1 enable command logging

Purpose

To enable the command logging function.

Format

enable command logging

Description

This command is used to enable the command logging function.

Note: When the Switch is under the booting procedure and the procedure of downloading the configuration to execute immediately, all configuration commands should not be logged. When the user is under AAA authentication, the user name should not changed if user uses “enable admin” command to replace its privilege.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the command logging function:

```
DGS-3200-10:4# enable command logging
Command: enable command logging

Success.

DGS-3200-10:4#
```

19-2 disable command logging

Purpose

To disable the command logging function.

Format

disable command logging

Description

This command is used to disable the command logging function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the command logging:

```
DGS-3200-10:4# disable command logging
Command: disable command logging

Success.

DGS-3200-10:4#
```

19-3 show command logging

Purpose

To display the Switch's general command logging configuration status.

Format

show command logging

Description

This command is used to display the Switch's general command logging configuration status.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the command logging configuration status:

```
DGS-3200-10:4# show command logging
Command: show command logging


Command Logging State : Disabled


DGS-3200-10:4#
```

20 Modify Banner and Prompt Command List

config greeting_message {default}
config command_prompt [<string 16> | username | default]

20-1 config greeting_message

Purpose

To configure the greeting message(or banner).

Format

config greeting_message {default}

Description

This command is used to modify the login banner.

Parameters

Parameters	Description
default	Adding this parameter to the **config greeting_message** command will return the greeting message (banner) to its original factory default entry.

Restrictions

1. When users issue the “reset” command, the modified banner will remain in tact. Yet, issuing the “reset system” will return the banner to its original default value.
2. The maximum character capacity for the banner is 24*80. (24 Lines and 80 characters per line)
3. In the following example, Ctrl+W will save the modified banner only to the DRAM. Users must enter the “save” command to save this entry to the FLASH memory.
4. Only Administrator-level users can issue this command.

Example

To edit the banner:

```
DGS-3200-10:4#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================

                        DGS-3200-10 Gigabit Ethernet Switch
                              Command Line Interface

                             Firmware: Build 2.00.012
           Copyright(C) 2011 D-Link Corporation. All rights reserved.
================================================================================

   <Function Key>                    <Control Key>
   Ctrl+C     Quit without save      left/right/
   Ctrl+W     Save and quit            up/down     Move cursor
                                       Ctrl+D        Delete line
                                       Ctrl+X        Erase all setting
                                       Ctrl+L        Reload original setting
--------------------------------------------------------------------------------

Success.

DGS-3200-10:4#
```

20-2 config command_prompt

Purpose

To configure the command prompt.

Format

config command_prompt [<string 16> | username | default]

Description

This command is used to modify the command prompt.

The current command prompt consists of four parts: “product name” + “:” + ”user level” + ”#” (e.g. “**DGS-3200-10:4#**”). This command is used to modify the first part (1. “product name”) with a string consisting of a maximum of 16 characters, or to be replaced with the users’ login user name.

Parameters

Parameters	Description
string	Enter the new command prompt string of no more than 16 characters.
username	Enter this command to set the login username as the command prompt.
default	Enter this command to return the command prompt to its original factory default value.

Restrictions

1. When users issue the “reset” command, the current command prompt will remain in tact. Yet, issuing the “reset system” will return the command prompt to its original factory default value.
2. Only Administrator-level users can issue this command.

Example

To edit the command prompt:

```
DGS-3200-10:4#config command_prompt DGS-3200-10
Command: config command_prompt DGS-3200-10

Success.

DGS-3200-10:4#
```

21 SMTP Command List

enable smtp
disable smtp
config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}
show smtp
smtp send_testmsg

21-1 enable smtp

Purpose

To enable SMTP status.

Format

enable smtp

Description

This command is used to enable the SMTP status.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SMTP status:

```
DES-3200-10:4#enable smtp
Command: enable smtp


Success.


DES-3200-10:4#
```

21-2 disable smtp

Purpose

To disable SMTP status.

Format

disable smtp

Description

This command is used to disable SMTP status.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SMTP status:

```
DES-3200-10:4#disable smtp
Command: disable smtp

Success.

DES-3200-10:4#
```

21-3 config smtp

Purpose

To configure SMTP settings.

Format

config smtp {server <ipaddr> | server_port <tcp_port_number 1-65535> | self_mail_addr <mail_addr 64> | [add mail_receiver <mail_addr 64> | delete mail_receiver <index 1-8>]}

Description

This command is used to configure SMTP settings.

Parameters

Parameters	Description
server	Specifies the SMTP server IP address.
server_port	Specifies the SMTP server port.
self_mail_addr	Specifiles the sender's mail address.
add mail_receiver	Add mail receiver's address.
delete mail_receiver	Delete mail receiver's address.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure a SMTP server IP address:

```
DES-3200-10:4#config smtp server 172.18.208.9
Command: config smtp server 172.18.208.9

Success.

DES-3200-10:4#
```

To configure an SMTP server port:

```
DES-3200-10:4#config smtp server_port 25
Command: config smtp server_port 25

Success.

DES-3200-10:4##
```

To configure a mail source address:

```
DES-3200-10:4#config smtp self_mail_addr mail@dlink.com
Command: config smtp self_mail_addr mail@dlink.com

Success.

DES-3200-10:4#
```

To add a mail destination address:

```
DES-3200-10:4#config smtp add mail_receiver receiver@dlink.com
Command: config smtp add mail_receiver receiver@dlink.com

Success.

DES-3200-10:4#
```

To delete a mail destination address:

```
DES-3200-10:4#config smtp delete mail_receiver 1
Command: config smtp delete mail_receiver 1


Success.


DES-3200-10:4#
```

21-4 show smtp

Purpose

To display the current SMTP information.

Format

show smtp

Description

This command is display the current SMTP information.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the current SMTP information:

```
DES-3200-10:4#show smtp
Command: show smtp

SMTP Status              : Enabled
SMTP Server Address      : 172.18.208.9
SMTP Server Port         : 25
Self Mail Address        : mail@dlink.com

Index    Mail Receiver Address
-----    ------------------------------------------------------------------------

1        receiver@dlink.com
2
3
4
5
6
7
8

DES-3200-10:4#6
```

21-5 smtp send_testmsg

Purpose

To test whether the SMTP server can be reached.

Format

smtp send_testmsg

Description

This command is used to test whether the SMTP server can be reached.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To test whether the SMTP server can be reached:

Note: The sentences following “Subject:” and “Content:” are user inputs.

```
DES-3200-10:4#smtp send_testmsg
Command: smtp send_testmsg

Subject:Here the user can enter the subject
Content:Here the user can enter the content

Sending mail,please wait...
Success.

DES-3200-10:4#
```

22 Time and SNTP Command List

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}
show sntp
enable sntp
disable sntp
config time <date ddmmmyyyy > <time hh:mm:ss >
config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst [disable **| repeating {s_week <start_week 1-4,last>** **| s_wday <start_day sun-sat>** **| s_mth <start_mth 1-12>** **| s_time <start_time hh:mm>** **| e_week <end_week 1-4,last>** **| e_wday <end_day sun-sat>** **| e_mth <end_mth 1-12>** **| e_time <end_time hh:mm>** **| offset [30 | 60|90|120]}** **| annual {s_date <start_date 1-31>** **| s_mth <start_mth 1-12>** **| s_time <start_time hh:mm>** **| e_date <end_date 1-31>** **| e_mth <end_mth 1-12>** **| e_time <end_time hh:mm>** **| offset [30 | 60 | 90 | 120]}]**
show time

22-1 config sntp

Purpose

To configure SNTP.

Format

config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}

Description

This command is used to change SNTP configurations.

Parameters

Parameters	Description
primary	The SNTP primary server IP address.
secondary	The SNTP secondary server IP address.
poll-interval	The polling interval range is between 30 and 99999 seconds.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure SNTP:

```
DGS-3200-10:4#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DGS-3200-10:4#
```

22-2 show sntp

Purpose

To display SNTP configuration.

Format

show sntp

Description

This command is used to display the current SNTP time source and configuration.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show SNTP:

```
DGS-3200-10:4#show sntp
Command: show sntp

Current Time Source   : System Clock
SNTP                  : Disabled
SNTP Primary Server   : 10.1.1.1
SNTP Secondary Server : 10.1.1.2
SNTP Poll Interval    : 30 sec

DGS-3200-10:4#
```

22-3 enable sntp

Purpose

To turn on SNTP support.

Format

enable sntp

Description

This command is used to turn on SNTP support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable SNTP:

```
DGS-3200-10:4#enable sntp
Command: enable sntp

Success.

DGS-3200-10:4#
```

22-4 disable sntp

Purpose

To turn off SNTP support.

Format

disable sntp

Description

This command is used to turn off SNTP support.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable SNTP:

```
DGS-3200-10:4#disable sntp
Command: disable sntp

Success.

DGS-3200-10:4#
```

22-5 config time

Purpose

To configure the time and date settings of the device.

Format

config time <date ddmthyyyy> <time hh:mm:ss>

Description

This command is used to change the time settings.

Parameters

Parameters	Description
date	The system clock date.
time	The system clock time.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the time:

```
DGS-3200-10:4# config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3200-10:4#
```

22-6 config time_zone

Purpose

To configure the time zone of the device.

Format

config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}

Description

This command is used to change time zone settings.

Parameters

Parameters	Description
operator	The operator of the time zone. + : positive - : negative.
hour	The hour setting of the time zone.
min	The minute setting of the time zone.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the time zone:

```
DGS-3200-10:4#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3200-10:4#
```

22-7 config dst

Purpose

To configure Daylight Saving Time on the device.

Format

config dst [disable | repeating {s-week <start_week 1-4,last> | s-day <start_weekday sun-sat> | s-mth <start_mth 1-12> | s-time <start_time hh:mm> | e-week <end_week 1-4,last> | e-day <end_weekday sun-sat> | e-mth <end_mth 1-12> | e-time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s-date <start_date 1-31> | s-mth <start_mth 1-12> | s-time <start_time hh:mm> | e-date <end_date 1-31> | e-mth <end_mth 1-12> | e-time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]

Description

This command is used to configure Daylight Saving Time settings.

Parameters

Parameters	Description
disable	Disable the DST of the switch .
repeating	Set the DST to repeating mode .
annual	Set the DST to annual mode.
s_week, e_week	Configure the start/end week number of DST.
s_day, e_day	Configure the start/end day number of DST.
s_mth, e_mth	Configure the start/end month number of DST.
s_time, e_time	Configure the start/end time of DST.
s_date, e_date	Configure the start/end date of DST
offset	Indicate the number of minutes to add or to subtract during summertime. The range of offsets are 30, 60, 90, and 120. The default value is 60.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure daylight saving time to start on the second week, on Tuesday, in April, at 15:00 and end on the second week, on Wednesday, in October, at 15:30:

```
DGS-3200-10:4#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week
 2 e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e
_day wed e_mth 10 e_time 15:30 offset 30
```

```
Success.


DGS-3200-10:4#
```

22-8 show time

Purpose

To display time states.

Format

show time

Description

This command is used to display current time states.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show the current time settings:

```
DGS-3200-10:4#show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 1 Jan 2000  00:00:00
     Current Time : 1 Jan 2000  07:26:28
     Time Zone    : GMT +00:00
     Daylight Saving Time : Disabled
          Offset in Minutes: 60
          Repeating From   : Apr 2nd  Tue 15:00
                     To     : Oct last Sun 00:00
          Annual    From   : 29 Apr 00:00
                     To     : 12 Oct 00:00
DGS-3200-10:4#
```

23 Jumbo Frame Command List

enable jumbo_frame
disable jumbo_frame
show jumbo_frame

23-1 enable jumbo_frame

Purpose

To enable support of Jumbo Frames.

Format

enable jumbo_frame

Description

This command is used to enable support of Jumbo Frames.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable Jumbo Frames:

```
DGS-3200-10:4#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of Jumbo Frame is 10240 Bytes.
Success.

DGS-3200-10:4#
```

23-2 disable jumbo_frame

Purpose

To disable support of Jumbo Frames.

Format

disable jumbo_frame

Description

This command is used to disable support of Jumbo Frames.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable Jumbo Frames:

```
DGS-3200-10:4#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3200-10:4#
```

23-3 show jumbo_frame

Purpose

To display the Jumbo Frames configuration.

Format

show jumbo_frame

Description

This command is used to display the Jumbo Frames configuration.

Parameters

None.

Restrictions

None.

Example

To display the Jumbo Frames configuration:

```
DGS-3200-10:4#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Disabled
Maximum Frame Size : 1536 Bytes

DGS-3200-10:4#
```

24 Single IP Management Command List

enable sim
disable sim
show sim { [candidates { <candidate_id 1-100> } | members { <member_id 1-32> } | group {commander_mac <macaddr>} | neighbor] }
reconfig { member_id <value 1-32> | exit }
config sim_group [add <candidate_id 1-100> { <password> } | delete <member_id 1-32>]
config sim [[commander { group_name <groupname 64> } | candidate] | dp_interval <sec 30-90> | hold_time <sec 100-255>]
download sim_ms [firmware_from_tftp | configuration_from_tftp] {<ipaddr> <path_filename> {[members <mslist 1-32> | all]}}
upload sim_ms [configuration_to_tftp | log_to_tftp] {<ipaddr> <path_filename> {members <mslist> | all}}
config sim trap [enable | disable]

24-1 enable sim

Purpose

To enable single IP management.

Format

enable sim

Description

This command is used to configure the single IP management on the switch as enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable single IP management:

```
DGS-3200-10:4#enable sim
Command: enable sim

Success.

DGS-3200-10:4#
```

24-2 disable sim

Purpose

To disable single IP management on the switch.

Format

disable sim

Description

This command is used to configure the single IP management on the switch as disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable single IP management:

```
DGS-3200-10:4#disable
Command: disable sim

Success.

DGS-3200-10:4#
```

24-3 show sim

Purpose

To display the current information of the specific sorts of devices.

Format

show sim { [candidates { <candidate_id 1-100> } | members { <member_id 1-32> } | group {commander_mac <macaddr>} | neighbor] }

Description

This command is used to display the information of the specific sorts of devices including of self, candidate, member, group, and neighbor.

Parameters

Parameters	Description
candidates	Specify the candidate devices.
members	Specify the member devices.
group	Specify other group devices.
neighbor	Specify other neighbor devices.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the self information in detail:

```
DGS-3200-10:4#show sim
Command: show sim

SIM Version         : VER-1.61
Firmware Version    : Build 1.50.B008
Device Name         :
MAC Address         : 00-35-26-11-11-00
Capabilities        : L2
Platform            : DGS-3200-10 L2 Switch
SIM State           : Disabled
Role State          : Candidate
Discovery Interval : 30 sec
Hold Time           : 100 sec
Trap                : Enabled

DGS-3200-10:4#
```

To show the candidate information in summary:

```
DGS-3200-10:4#show sim candidate
Command: show sim candidate

ID  MAC Address       Platform /                Hold  Firmware Device Name
                      Capability                Time  Version
--- ----------------- ------------------------- ----- --------- ----------------
 1  00-01-02-03-04-00 DGS-3200-10 L2 Switch      40   1.50-B008 aaaaaaaaaaaaaaa
                                                                 bbbbbbbbbbbbbb
 2  00-55-55-00-55-00 DES-3326SR L3 Switch      140   4.00-B15 default master

Total Entries: 2

DGS-3200-10:4#
```

To show the member information in summary:

```
DGS-3200-10:4#show sim member
Command: show sim member

ID  MAC Address       Platform /                Hold  Firmware Device Name
                      Capability                Time  Version
--- ----------------- ------------------------- ----- --------- ----------------
1  00-01-02-03-04-00 DGS-3200-10 L2 Switch      40   1.50-B008 aaaaaaaaaaaaaaa
                                                                 bbbbbbbbbbbbbb
2  00-55-55-00-55-00 DES-3326SR L3 Switch      140   4.00-B15 default master

Total Entries: 2

DGS-3200-10:4#
```

To show other groups information in summary:

```
DGS-3200-10:4#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address       Platform /                Hold  Firmware Device Name
Capability                Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
*1  00-01-02-03-04-00 DGS-3200-10 L2 Switch      40   1.50-B008 aaaaaaaaaaaaaaa
                                                                bbbbbbbbbbbbbb
 2  00-55-55-00-55-00

SIM Group Name : SIM2

ID  MAC Address       Platform /                Hold  Firmware Device Name
Capability                Time  Version
--- ----------------- ------------------------ ----- --------- ----------------
*1  00-01-02-03-04-00 DGS-3200-10 L2 Switch      40   1.50-B008 aaaaaaaaaaaaaaa
                                                                bbbbbbbbbbbbbb
 2  00-55-55-00-55-00

‘*’ means commander switch.

DGS-3200-10:4#
```

To show an SIM neighbor table:

```
DGS-3200-10:4# show sim neighbor
Command: show sim neighbor

Neighbor Table

Port     MAC Address          Role
------   ------------------   ---------
23       00-35-26-00-11-99    Commander
23       00-35-26-00-11-91    Member
24       00-35-26-00-11-90    Candidate

Total Entries: 3

DGS-3200-10:4#
```

24-4 reconfig

Purpose

To re-Telnet to a member.

Format

reconfig { member_id <value 1-32> | exit }

Description

This command is used to re-Telnet to a member.

Parameters

Parameters	Description
member_id	Specify the serial number of a member.

Restrictions

Only Administrator-level users can issue this command.

Examples

To re-Telnet to a member:

```
DGS-3200-10:4#reconfig member_id 1
Command: reconfig member_id 1

DGS-3200-10:4#
Login:
```

24-5 config sim_group

Purpose

To configure group information.

Format

config sim_group [add <candidate_id 1-100> { <password> } | delete <member_id 1-32>]

Description

This command is used to configure group information on the switch.

Parameters

Parameters	Description
candidate_id	Add a specific candidate to group.
password	The password of candidate if necessary.
member_id	Remove a specific member from group.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a member:

```
DGS-3200-10:4# config sim_group add 2
Command: config sim_group add 2

Please wait for ACK !!!
SIM Config Success !!!

Success.

DGS-3200-10:4#
```

To delete a member:

```
DGS-3200-10:4# config sim_group delete 1
Command: config sim_group delete 1

Please wait for ACK !!!
SIM Config Success !!!

Success.
DGS-3200-10:4#
```

24-6 config sim

Purpose

To configure the role state and parameters of discovery protocol on the switch.

Format

config sim [[commander { group_name <groupname 64> } | candidate] |dp_interval <sec 30-90> | hold_time <sec 100-255>]

Description

This command is used to configure the role state and parameters of discovery protocol on the switch.

Parameters

Parameters	Description
commander	Transfer role to commander.
group_name	If commander, a user can update the name of a group.
candidate	Transfer role to candidate.
dp_interval	The time in seconds between discovery.
hold_time	The time in seconds the device holds the discovery result.

Restrictions

Only Administrator-level users can issue this command.

Examples

To transfer to commander:

```
DGS-3200-10:4# config sim commander
Command: config sim commander

Success.

DGS-3200-10:4#
```

To transfer to candidate:

```
DGS-3200-10:4# config sim candidate
Command: config sim candidate

Success.

DGS-3200-10:4#
```

To update name of group:

```
DGS-3200-10:4#config sim commander group_name mygroup
Command: config sim commander group_name mygroup

Success.

DGS-3200-10:4#
```

To change the time interval of discovery protocol:

```
DGS-3200-10:4# config sim dp_interval 30
Command: config sim dp_interval 30

Success.

DGS-3200-10:4#
```

To change the hold time of discovery protocol:

```
DGS-3200-10:4# config sim hold_time 200
Command: config sim hold_time 200

Success.

DGS-3200-10:4#
```

24-7 download sim_ms

Purpose

To download firmware or configuration to indicated device.

Format

download sim_ms [firmware_from_tftp | configuration_from_tftp] {<ipaddr> <path_filename>

{[members <mslist 1-32> | all]}}

Description

This command is used to download firmware or configuration from a TFTP server to indicated devices.

Parameters

Parameters	Description
firmware_from_tftp	Specify to download firmware from a TFTP server.
configuration_from_tftp	Specify to download configuration from a TFTP server.
<ipaddr>	Specify the IP address of a TFTP server.
<path_filename>	Specify the file path of firmware or configuration to be sent to a TFTP server.
members	Specify a range of members which can download this firmware or configuration.
all	Specify all members which download this firmware or configuration.

Restrictions

Only Administrator-level users can issue this command.

Examples

To download firmware:

```
DGS-3200-10:4# download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1
Commands: download sim_ms configuration_from_tftp 10.55.47.1 D:\dwl600x.tfp
members 1

This device is updating firmware.  Please wait...

Download Status :

ID   MAC Address         Result
---  ------------------  ----------------
1    00-01-02-03-04-00   Success
2    00-07-06-05-04-03   Fail
3    00-07-06-05-04-04   Fail

DGS-3200-10:4#
```

To download configuration:

```
DGS-3200-10:4# download sim_ms configuratin_from_tftp 10.55.47.1 D:\test.txt 1
Commands: download sim_ms configuratin_from_tftp 10.55.47.1 D:\test.txt 1
<new page>

This device is updating configuration.  Please wait...

Download Status :

ID   MAC Address         Result
---  ----------------  ---------------
1   00-01-02-03-04-00  Success
2   00-07-06-05-04-03  Fail
3   00-07-06-05-04-03  Fail

DGS-3200-10:4#
```

24-8 upload sim_ms

Purpose

To upload a configuration file to a TFTP server.

Format

upload sim_ms [configuration_to_tftp | log_to_tftp] {<ipaddr> <path_filename> {members <mslist> | all}}

Description

This command is used to upload a configuration file from indicated devices to a TFTP server.

Parameters

Parameters	Description
configuration_to_ftp	Specify to upload configuration to a TFTP server.
log_to_tftp	Specify to upload a log to a TFTP server.
<ipaddr>	Specify the IP address of a TFTP server.
<path_filename>	Specify the file path to store a configuration file to be sent to a TFTP server.
members	Specify the member which can upload its configuration file.
all	Specify all members which upload its configuration.

Restrictions

Only Administrator-level users can issue this command.

Examples

To upload a configuration file:

```
DGS-3200-10:4#upload sim_ms configuration_to_tftp 10.55.47.1
D:\configuration.txt members 1
Command: upload sim_ms configuration_to_tftp 10.55.47.1 D:\configuration.txt
members 1

Done.

DGS-3200-10:4#
```

24-9 config sim trap

Purpose

To control sending of traps issued from the member switch.

Format

config sim trap [enable | disable]

Description

This command is used to control the sending of traps issued from a member switch.

Parameters

Parameters	Description
trap	Enable or disable the trap state. The default state is enable.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable a SIM trap:

```
DGS-3200-10:4#config sim trap disable
Command: config sim trap disable

Success.

DGS-3200-10:4#
```

25 Safeguard Engine Command List

config safeguard_engine { state [enable | disable] | utilization{rising <value 20-100> | falling <value 20-100>}| trap_log [enable | disable] | mode [strict | fuzzy]}
show safeguard_engine

25-1 config safeguard_engine

Purpose

To configure the safeguard engine.

Format

config safeguard_engine { state [enable | disable] | utilization{rising <value 20-100> | falling <value 20-100>}| trap_log [enable | disable] | mode [strict | fuzzy]}

Description

Use this command to configure the safeguard engine for the system.

Parameters

Parameters	Description
state	Configure the safeguard engine state to **enable** or **disable**.
trap_log	Configure the state of safeguard engine related trap/log mechanism to **enable** or **disable**. If set to **enable**, trap and log will be active while the safeguard engine current mode is changed. If set to **disable**, current mode change will not trigger trap and log events.
mode	Determine the controlling method of broadcast traffic. Here are two modes (**strict** and **fuzzy**). In **strict**, the Switch will stop receiving all 'ARP not to me' packets (the protocol address of target in ARP packet is the Switch itself). That means no matter what reasons cause the high CPU utilization (may not caused by ARP storm), the Switch reluctantly processes any 'ARP not to me' packets in exhausted mode. In **fuzzy** mode, the Switch will adjust the bandwidth dynamically depend on some reasonable algorithm.
utilization	Configure the safeguard engine threshold.

	rising	Configure the utilization rising threshold. The range is between 20%-100%. If the CPU utilization is over the rising threshold, the switch enters exhausted mode.
	falling	Configure the utilization falling threshold. The range is between 20%-100%. If the CPU utilization is lower than the falling threshold, the switch enters normal mode.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the safeguard engine:

```
DGS-3200-10:4#config safeguard_engine state enable utilization rising 50 falling
30 trap_log enable
Command: config safeguard_engine state enable utilization rising 50 falling 30
trap_log enable

Success.

DGS-3200-10:4#
```

25-2 show safeguard_engine

Purpose

To show safeguard engine information.

Format

show safeguard_engine

Description

Use this command to display safeguard engine information.

Parameters

None.

Restrictions

None.

Examples

To display safeguard engine information:

```
DGS-3200-10:4#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State          : Disabled
Safeguard Engine Current Status : Normal Mode
================================================
CPU Utilization Information:
Rising Threshold  :  30%
Falling Threshold :  20%
Trap/Log State    :  Disabled
Mode              :  Fuzzy

DGS-3200-10:4#
```

Note: The safeguard engine current status has two modes: exhausted and normal mode.

26 Debug Software Command List

debug address_binding [event |dhcp |all] state [enable|disable]
no debug address_binding
debug show address_binding binding_state_table [nd_snooping | dhcpv6_snooping]
debug error_log [dump | clear | upload_toTFTP {<ipaddr> <path_filename 64>}]
debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]
debug output [module <module_list> | all] [buffer | console]
debug config error_reboot [enable | disable]
debug show status {module <module_list>}
debug config state [enable | disable]
debug show error_reboot state
debug dhcpv6_client state enable
debug dhcpv6_client state disable
debug dhcpv6_client output [buffer | console]
debug dhcpv6_client packet [all | receiving | sending] state [enable | disable]
debug dhcpv6_relay state enable
debug dhcpv6_relay state disable
debug dhcpv6_relay output [buffer | console]
debug dhcpv6_relay packet [all | receiving | sending] state [enable | disable]
debug dhcpv6_relay hop_count state [enable | disable]

26-1 debug address_binding

Purpose

To start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

debug address_binding [event |dhcp |all] state [enable|disable]

Description

This command is used to start the IMPB debug when the IMPB module receives an ARP/IP packet or a DHCP packet.

Parameters

Parameters	Description
event	Specify to display the debug messages when the IMPB module

	receives ARP/IP packets.
dhcp	Specify to display the debug messages when the IMPB module receives DHCP packets.
all	Specify to display all debug messages.
state	Enable or disable the IMPB debug state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To print out all debug IMPB messages:

```
DGS-3200-10:4# debug address_binding all state enable
Command: debug address_binding all state enable

Success.

DGS-3200-10:4#
```

26-2 no debug address_binding

Purpose

To stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.

Format

no debug address_binding

Description

This command is used to stop the IMPB debug starting when the IMPB module receives an ARP/IP packet or a DHCP packet.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To stop IMPB debug: starting when the IMPB module receives an ARP/IP or DHCP packet:

```
DGS-3200-10:4# no debug address_binding
Command: no debug address_binding

Success.
```

```
DGS-3200-10:4#
```

26-3 debug show address_binding binding_state_table

Purpose

To show the binding state of the entries in the BST.

Format

debug show address_binding binding_state_table [nd_snooping | dhcpv6_snooping]

Description

The command is used to show the ND snooping and DHCPv6 BST (Binding State Table).

Parameters

Parameters	Description
nd_snooping	Specify to display the ND snooping BST.
dhcpv6_snooping	Specify to display the DHCPv6 snooping BST.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the DHCPv6 snooping binding state of entries in BST:

```
DGS-3200-10:4# debug show address_binding binding_state_table dhcpv6_snooping
Command:debug show address_binding binding_state_table dhcpv6_snooping
S (State) – S: Start, L: Live, D :Detection, R: Renew, B: Bound
Time – Expiry Time (sec)

IP Address                              MAC Address         S   Time        Port
--------------------------------------- ------------------ -- ----------- ------
2001:2222:1111:7777:5555:6666:7777:8888 00-00-00-00-00-02   S  50           5
2001::1                                 00-00-00-00-03-02   B  100          6

Total entries : 2

DGS-3200-10:4#
```

26-4 debug error_log

Purpose

To dump, clear or upload the software error log to a TFTP server.

Format

debug error_log [dump | clear | upload_toTFTP {<ipaddr> <path_filename 64>}]

Description

This command is used to dump, clear or upload the software error log to a TFTP server.

Parameters

Parameters	Description
dump	Display the debug message of the debug log.
clear	Clear the debug log.
upload_toTFTP	pload the debug log to a TFTP server specified by IP address.
<ipaddr>	Specify the IPv4 address of the TFTP server.
<path_filename 64>	The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrator-level users can issue this command.

Examples

To dump the error log:

```
DGS-3200-10:4#debug error_log dump
Command: debug error_log dump


********************************************************************************
# debug log: 1
# firmware version: 1.00.011
# level: CPU exception
# clock: 437453880 ms
# time : 2000-01-08 05:55:40


======================= CPU EXCEPTION ========================
Current Task = IP-Tic Stack Pointer = 4CFEA7A0
--------------------------CP0 Registers----------------------
Status : 1000FC01  Interrupt enable  Normal level
Cause  : 00000008  TLB exception (load or instruction fetch)
```

```
EPC   : 80A0297C      Addr   : 00000008
Stack  : 4CFEA7A0      Return : 80A02938
------------------------normal registers-----------------------
$0( $0) : 00000000  at( $1) : FFFFFFFE  v0( $2) : 00000000  v1( $3) : 00000001
a0( $4) : 00000000  a1( $5) : 4825B4A8  a2( $6) : 00000001  a3( $7) : 00000001
t0( $8) : 814D7FCC  t1( $9) : 0000FC00  t2($10) : 828100C4  t3($11) : 00000017
t4($12) : 828100BC  t5($13) : 4CFEA430  t6($14) : 82810048  t7($15) : 00000000
s0($16) : 4825D94A  s1($17) : 4825D890  s2($18) : 4825D949  s3($19) : 4825D946
s4($20) : 00000000  s5($21) : 00000008  s6($22) : 81800000  s7($23) : 00090000
t8($24) : 00000000  t9($25) : FFFFFFC0  k0($26) : 00000000  k1($27) : 00000000
gp($28) : 8180ADA0  sp($29) : 4CFEA7A0  fp($30) : 00000001  ra($31) : 80A02938



------------------------ TASK STACKTRACE -----------------------
->81150A58
->809B346C
->809E1DEC
->809D7E6C
->80A038CC
->80A033B0
->80A0297C

DGS-3200-10:4#
```

To clear the error log:

```
DGS-3200-10:4# debug error_log clear
Command: debug error_log clear

Success.

DGS-3200-10:4#
```

To upload the error log to TFTP server:

```
DGS-3200-10:4# debug error_log upload_toTFTP 10.0.0.90 debug-log.txt
Command: debug error_log upload_toTFTP 10.0.0.90 debug-log.txt

Connecting to server.................. Done.
Upload configuration.................. Done.

DGS-3200-10:4#
```

26-5 debug buffer

Purpose

To show the debug buffer's state, or dump, clear, or upload the debug buffer to a TFTP server.

Format

debug buffer [utilization | dump | clear | upload_toTFTP <ipaddr> <path_filename 64>]

Description

This command is used to show the debug buffer's state, or dump, clear, or upload the debug buffer to a TFTP server.

Note: When selecting to output to the debug buffer and there are debug messages being outputted, the system memory pool will be used as the debug buffer. The functions which will use the system memory pool resource may fail to execute command such as download and upload firmware, or save configuration. If you want to execute these commands successfully, use the command **debug buffer clear** to release the system's memory pool resources manually first.

Parameters

Parameters	Description
utilization	Display the debug buffer's state.
dump	Display the debug message in the debug buffer.
clear	Clear the debug buffer.
upload_toTFTP	Upload the debug buffer to a TFTP server specified by IP address.
<ipaddr>	Specify the IPv4 address of the TFTP server.
<path_filename 64>	The pathname specifies the DOS pathname on the TFTP server. It can be a relative pathname or an absolute pathname. This value can be up to 64 characters long.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the debug buffer's state:

```
DGS-3200-10:4# debug buffer utilization
Command: debug buffer utilization

Allocate from:    System memory
Total size   :    2 MB
Utilization rate  :    30%

DGS-3200-10:4#
```

To clear the debug buffer:

```
DGS-3200-10:4# debug buffer clear
Command: debug buffer clear

Success.

DGS-3200-10:4#
```

To upload the messages stored in debug buffer to TFTP server:

```
DGS-3200-10:4# debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt
Command: debug buffer upload_toTFTP 10.0.0.90 debugcontent.txt

Connecting to server................... Done.
Upload configuration................... Done.

DGS-3200-10:4#
```

26-6 debug output

Purpose

To set a specified module's debug message output to debug buffer or local console. If the user uses the command in a Telnet session, the error message also is output to the local console.

Format

debug output [module <module_list> | all] [buffer | console]

Description

This command is used to set a specified module's debug message output to debug buffer or local console.

If the user uses the command in a Telnet session, the error message also is output to the local console.
Note: When selecting to output to the debug buffer and there are debug messages being outputted, the system memory pool will be used as the debug buffer. The functions which will use the system memory pool resource may fail to execute command such as download and upload firmware, or save configuration. If you want to execute these commands successfully, please use the command “debug buffer clear” to release the system’s memory pool resources manually first.

Parameters

Parameters	Description
<module_list>	Specify the module list.
all	Control output method of all modules.
buffer	Direct the debug message of the module output to debug buffer(default).
console	Direct the debug message of the module output to local console.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set all module debug message outputs to local console:

```
DGS-3200-10:4# debug output all console
Command: debug output all console

Success.

DGS-3200-10:4#
```

26-7 debug config error_reboot

Purpose

To set if the switch needs to be rebooted when a fatal error occurs.

Format

debug config error_reboot [enable | disable]

Description

This command is used to set if the switch needs to be rebooted when a fatal error occurs. When the error occurs, the watchdog timer will be disabled by the system first, and then all debug information will be saved in NVRAM. If the error_reboot is enabled, the watchdog shall be enabled after all information is stored into NVRAM.

Parameters

Parameters	Description
enable	Need to reboot the Switch when fatal error happens.
disable	Do not need to reboot the Switch when fatal error happens. The system will hang-up for debug and enter the debug shell mode for debug.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the switch to not need a reboot when a fatal error occurs:

```
DGS-3200-10:4#debug config error_reboot disable
Command: debug config error_reboot disable

Success.

DGS-3200-10:4#
```

26-8 debug show status

Purpose

To show the specified module's debug status.

Format

debug show status {module <module_list>}

Description

This command is used to show the debug handler state and the specified module's debug status.
If the input module list is empty, the states of all registered modules which support debug module will be shown.

Parameters

Parameters	Description
<module_list>	Specify the module lilst.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the specified module's debug state:

```
DGS-3200-10:4#debug show status module MSTP
Command: debug show status module MSTP

Debug Global State: Enabled

MSTP    : Enabled



DGS-3200-10:4#
```

To show the debug state:

```
DGS-3200-10:4#debug show status
Command: debug show status

Debug Global State  : Disabled

IMPB                : Disabled
DHCPv6_RELAY        : Disabled

DGS-3200-10:4#
```

26-9 debug config state

Purpose

To set the state of the debug.

Format

debug config state [enable | disable]

Description

This command is used to set the state of the debug.

Parameters

Parameters	Description
enable	Enable the debug state.
disable	Disable the debug state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the debug state to disabled:

```
DGS-3200-10:4#debug config state disable
Command: debug config state disable

Success.

DGS-3200-10:4#
```

26-10 debug show error_reboot state

Purpose

To show the error reboot status.

Format

debug show error_reboot state

Description

This command is used to show the error reboot status.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the error reboot status.

```
DGS-3200-10:4#debug show error_reboot state
Command: debug show error_reboot state

Error Reboot: Enabled

DGS-3200-10:4#
```

26-11 debug dhcpv6_client state enable

Purpose

To enable the DHCPv6 client debug function.

Format

debug dhcpv6_client state enable

Description

This command is used to enable the DHCPv6 client debug function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enabled the DHCPv6 client debug function:

```
DGS-3200-10:4#debug dhcpv6_client state enable
Command: debug dhcpv6_client state enable


Success.


DGS-3200-10:4#
```

26-12 debug dhcpv6_client state disable

Purpose

To disable the DHCPv6 client debug function.

Format

debug dhcpv6_client state disable

Description

This command is used to disable the DHCPv6 client debug function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disabled the DHCPv6 client debug function:

```
DGS-3200-10:4#debug dhcpv6_client state disable
Command: debug dhcpv6_client state disable

Success.

DGS-3200-10:4#
```

26-13 debug dhcpv6_client output

Purpose

To set debug message to output to buffer or console.

Format

debug dhcpv6_client output [buffer | console]

Description

This command is used to set debug message to output to buffer or console.

Parameters

Parameters	Description
buffer	Let the debug message output to buffer.
console	Let the debug message output to console.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set debug information to output to console:

```
DGS-3200-10:4# debug dhcpv6_client output console
Command: debug dhcpv6_client output console

Success.

DGS-3200-10:4#
```

26-14 debug dhcpv6_client packet

Purpose

To enable or disable debug information flag for DHCPv6 client packet, including packet receiving and sending.

Format

debug dhcpv6_client packet [all | receiving | sending] state [enable | disable]

Description

This command is used to enable or disable debug information flag for DHCPv6 client packet, including packet receiving and sending.

Parameters

Parameters	Description
all	Set packet receiving and sending debug flags.
receiving	Set packet receiving debug flag.
sending	Set packet sending debug flag.
enable	Enable the designated flags.
disable	Disable the designated flags.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable DHCPv6client packet sending debug flags:

```
DGS-3200-10:4#debug dhcpv6_client packet sending state enable
Command: debug dhcpv6_client packet sending state enable

Success.

DGS-3200-10:4#
```

26-15 debug dhcpv6_relay state enable

Purpose

To enable DHCPv6 relay debug functions.

Format

debug dhcpv6_relay state enable

Description

This command is used to enable DHCPv6 relay debug functions.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enabled the DHCPv6 relay debug function:

```
DGS-3200-10:4#debug dhcpv6_relay state enable
Command: debug dhcpv6_relay state enable

Success.

DGS-3200-10:4#
```

26-16 debug dhcpv6_relay state disable

Purpose

To disable DHCPv6 relay debug functions.

Format

debug dhcpv6_relay state disable

Description

This command is used to disable DHCPv6 relay debug functions.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable DHCPv6 relay debug functions:

```
DGS-3200-10:4# debug dhcpv6_relay state disable
Command: debug dhcpv6_relay state disable

Success.

DGS-3200-10:4#
```

26-17 debug dhcpv6_relay output

Purpose

To set the debug message to output to a buffer or a console.

Format

debug dhcpv6_relay output [buffer | console]

Description

This command is used to set the debug message to output to a buffer or a console.

Parameters

Parameters	Description
buffer	Let the debug message output to buffer.
console	Let the debug message output to console.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set debug information to output to a console:

```
DGS-3200-10:4#debug dhcpv6_relay output console
Command: debug dhcpv6_relay output console

Success.

DGS-3200-10:4#
```

26-18 debug dhcpv6_relay packet

Purpose

To enable or disable the debug information flag of the DHCPv6 relay packet, including packets receiving and sending.

Format

debug dhcpv6_relay packet [all | receiving | sending] state [enable | disable]

Description

This command is used to enable or disable the debug information flag of the DHCPv6 relay packet, including packets receiving and sending.

Parameters

Parameters	Description
all	Set packet receiving and sending debug flags.
receiving	Set packet receiving debug flag.
sending	Set packet sending debug flag.
enable	Enable the designated flags.
disable	Disable the designated flags.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enabled the DHCPv6 relay packet sending debug:

```
DGS-3200-10:4#debug dhcpv6_relay packet sending state enable
Command: debug dhcpv6_relay packet sending state enable

Success.

DGS-3200-10:4#
```

26-19 debug dhcpv6_relay hop_count state

Purpose

To enable or disable debug information flag about the hop count.

Format

debug dhcpv6_relay hop_count state [enable | disable]

Description

This command is used to enable or disable debug information flag about the hop count.

Parameters

Parameters	Description
enable	Specify to enable the hop count state.
disable	Specify to disable the hop count state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable debug information flag about the hop count:

```
DGS-3200-10:4#debug dhcpv6_relay hop_count state enable
Command: debug dhcpv6_relay hop_count state enable

Success.

DGS-3200-10:4#
```

V. Layer 2

The Layer 2 section includes the following chapters: MSTP, FDB, MAC Notification, Mirror, VLAN/Protocol VLAN, VLAN Trunking, Link Aggregation, LACP Configuration, Traffic Segmentation, Port Security, Static MAC-based VLAN, and Port Egress Filter.

27 MSTP Command List

show stp
show stp instance {<value 0-15>}
show stp ports {<portlist>}
show stp mst_config_id
create stp instance_id <value 1-15>
delete stp instance_id <value 1-15>
config stp instance_id <value 1-15> [add_vlan|remove_vlan] <vidlist>
config stp mst_config_id {name <string> | revision_level <int>}
enable stp
disable stp
config stp version [mstp | rstp | stp]
config stp priority <value 0-61440> instance_id <value 0-15>
config stp {maxage <value 6-40> | **maxhops <value 6-40> |** **hellotime <value 1-2> |** **forwarddelay <value 4-30> |** **txholdcount <value 1-10> |** **fbpdu [enable | disable] | }**
config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | **hellotime <value 1-2> |** **migrate [yes | no] |** **edge [true | false | auto] |** **p2p [true | false | auto] |** **state [enable | disable] |** **restricted_role [true | false] |** **restricted_tcn [true | false] |** **fbpdu [enable | disable]}**
config stp mst_ports <portlist> instance_id <value 0-15> { internalCost [auto | <value

1-200000000>] | priority <value 0-240> }
config stp trap {new_root [enable|disable] | topo_change [enable | disable]}

27-1 show stp

Purpose

To display the MSTP information including parameter settings and operational values.

Format

show stp

Description

This command is used to display MSTP information including parameter settings and operational values.

Parameters

None.

Restrictions

None.

Examples

To display STP:

```
DGS-3200-10:4#show stp
Command: show stp

STP Bridge Global Settings
------------------------------
STP Status           : Enabled
STP Version          : MSTP
Max Age              : 20
Forward Delay        : 15
Max Hops             : 20
TX Hold Count        : 3
Forwarding BPDU      : Enabled
New Root Trap        : Enabled
Topology Change Trap: Disabled

DGS-3200-10:4#
```

27-2 show stp instance

Purpose

To display each instance parameter setting.

Format

show stp instance {<value 0-15>}

Description

This command is used to display each instance parameters settings. Value means the instance ID, if there is no input of this value, all instances will be shown.

Parameters

Parameters	Description
instance	MSTP instance ID. Instance 0 represents the default instance: CIST. The bridge supports a total 16 Instance（0-15）at most.

Restrictions

None.

Examples

To display STP instances:

```
DGS-3200-10:4#show stp instance
Command: show stp instance

STP Instance Settings
---------------------------
Instance Type           : CIST
Instance Status         : Enabled
Instance Priority       : 32768(bridge priority : 32768, sys ID ext : 0 )

STP Instance Operational Status
-------------------------------
Designated Root Bridge : 32768/00-22-22-22-22-00
External Root Cost     : 0
Regional Root Bridge   : 32768/00-22-22-22-22-00
Internal Root Cost     : 0
Designated Bridge      : 32768/00-22-22-22-22-00
Root Port              : None
Max Age                : 20
Forward Delay          : 15
```

```
Last Topology Change    : 2430
Topology Changes Count : 0


DGS-3200-10:4#
```

27-3 show stp ports

Purpose

To display port information including parameter settings and operational values.

Format

show stp ports {<portlist>}

Description

This command is used to display each port's parameter settings. If the portlist is not input, all ports will be shown. If there are multi instances on this bridge, the parameters of the port on different instances will be shown.

Parameters

Parameters	Description
ports	Show parameters of the designated port numbers which are distinguished from the parameters of the bridge.
portlist	One of the CLI Value Types, restricts the input value and format of the ports.

Restrictions

None.

Examples

To show STP ports:

```
DGS-3200-10:4#show stp ports
Command: show stp ports


MSTP Port Information
----------------------
Port Index      : 1      , Hello Time: 2 /2 , Port STP : Enabled  ,
External PathCost : Auto/200000   , Edge Port : False/No , P2P : Auto/Yes
Port RestrictedRole : False,  Port RestrictedTCN : False
Port Forward BPDU : Enabled
MSTI   Designated Bridge   Internal PathCost  Prio  Status      Role
-----  ------------------  -----------------  ----  ----------  ----------
```

```
0       N/A                  200000            128    Disabled    Disabled
2       N/A                  200000            128    Disabled    Disabled


DGS-3200-10:4#
```

27-4 show stp mst_config_id

Purpose

To display the MSTI configuration ID information including parameter settings and operational values.

Format

show stp mst_config_id

Description

This command is used to display the Configuration Name, Revision Level, MSTI ID, and the VID List. The default Configuration Name is the MAC address of the bridge.

Parameters

Parameters	Description
mst_config_id	If two bridges have the same three elements in **mst_config_id** , that means they are in the same MST region.

Restrictions

None.

Examples

To display the MST configuration ID:

```
DGS-3200-10:4#show stp mst_config_id
Command: show stp mst_config_id


Current MST Configuration Identification
---------------------------------------


Configuration Name : 00-22-22-22-22-00                        Revision Level :0
MSTI ID     Vid list
-------     ------------------------------------------------------------------
   CIST     1-4094


DGS-3200-10:4#
```

27-5 create stp instance_id

Purpose

To create an MST Instance without previously mapping the corresponding VLANs.

Format

create stp instance_id <value 1-15>

Description

This command is used to create an MSTI on the switch.

Parameters

Parameters	Description
instance_id	MSTP instance ID. Instance 0 represents a default instance, CIST. The DUT supports 16 Instance (0-15) at most.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an MSTP instance:

```
DGS-3200-10:4#create stp instance_id 2
Command: create stp instance_id 2

Success.

DGS-3200-10:4#
```

27-6 delete stp instance_id

Purpose

To delete an MST instance.

Format

delete stp instance_id <value 1-15>

Description

This command is used to delete the specified MST Instance. CIST（Instance 0）cannot be deleted and you can only delete one instance at a time.

Parameters

Parameters	Description

instance_id	MSTP instance ID. Instance 0 represents the default instance, CIST. The DUT supports 16 instances (0-15) at most.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an MSTP instance:

```
DGS-3200-10:4#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3200-10:4#
```

27-7 config stp instance_id

Purpose

To map or remove the VLAN range of the specified MST instance for an existing MST instance.

Format

config stp instance_id <value 1-15> [add_vlan|remove_vlan] <vidlist>

Description

There are two different action types to deal with an MST instance. They are listed as follows:

- **add_vlan**: To map specified VLAN lists to an existing MST instance..
- **remove_vlan**: To delete specified VLAN lists from an existing MST instance.

Parameters

Parameters	Description
instance_id	MSTP instance ID. Instance 0 represents a default instance, CIST. The DUT supports 16 instances (0-15) at most.
add_vlan	Specify the VLAN ID range from mapping MSTI add.
remove_vlan	Specify the VLAN ID range from mapping MSTI remove.
vidlist	Specify to assign the VLAN ID range.

Restrictions

Only Administrator-level users can issue this command.

Examples

To map a VLAN ID to an MSTP instance:

```
DGS-3200-10:4# config stp instance_id 2 add_vlan 1-3
Command: config stp instance_id 2 add_vlan 1-3

Success.

DGS-3200-10:4#
```

To remove a VLAN ID from an MSTP instance:

```
DGS-3200-10:4#config stp instance_id 2 remove_vlan 2
Command: config stp instance_id 2 remove_vlan 2

Success.

DGS-3200-10:4#
```

27-8 config stp mst_config_id

Purpose

To change the name or revision level of the MST configuration identification.

Format

config stp mst_config_id { name <string> | revision_level <int 0-65535> }

Description

This command is used to configure a configuration name or revision level in the MST configuration identification. The default configuration name is the MAC address of the bridge.

Parameters

Parameters	Description
name	The name given for a specified MST region.
revision_level	The same given name with a different revision level also represents a different MST region.

Restrictions

Only Administrator-level users can issue this command.

Examples

To change the name and revision level of the MST configuration identification:

```
DGS-3200-10:4#config stp mst_config_id name R&D_BlockG revision_level 1
Commands: config stp mst_config_id name R&D_BlockG revision_level 1

Success.

DGS-3200-10:4#
```

27-9 enable stp

Purpose

To enable STP globally.

Format

enable stp

Description

This command is used to enable STP. The default setting is disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable STP:

```
DGS-3200-10:4#enable stp
Command: enable stp

Success.

DGS-3200-10:4#
```

27-10 disable stp

Purpose

To disable STP globally.

Format

disable stp

Description

To disable STP functionality in every existing instance.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable STP:

```
DGS-3200-10:4#disable stp
Command: disable stp

Success.

DGS-3200-10:4#
```

27-11 config stp version

Purpose

To configure the STP run version.

Format

config stp version [mstp | rstp | stp]

Description

This command is used to configure the STP run version. The default setting is RSTP.

Parameters

Parameters	Description
version	To decide to run under which version of STP.
mstp	This stands for Multiple Spanning Tree Protocol.
rstp	This stands for Rapid Spanning Tree Protocol.
stp	This stands for Spanning Tree Protocol.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the STP version:

```
DGS-3200-10:4#config stp version mstp
Command: config stp version mstp

Success.

DGS-3200-10:4#
```

27-12 config stp priority

Purpose

To configure MSTI associate priority for the MSTP.

Format

config stp priority <value 0-61440> instance_id <value 0-15>

Description

This command is used to configure MSTI associate priority for the MSTP.

Parameters

Parameters	Description
priority	The bridge priority value must be divisible by 4096.
instance_id	An identifier to distinguish between different STP instances.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the STP instance ID:

```
DGS-3200-10:4#config stp priority 61440 instance_id 0
Command: config stp priority 61440 instance_id 0

Success.

DGS-3200-10:4#
```

27-13 config stp

Purpose

To configure the MSTP status on the switch.

Format

config stp { maxage <value 6-40> | maxhops <value 6-40> | hellotime <value 1-2> | forwarddelay <value 4-30> | txholdcount <value 1-10> | fbpdu [enable | disable]}

Description

This command is used to configure the MSTP status on the switch.

Parameters

Parameters	Description
maxage	Use to determine if a BPDU is valid. The default value is 20.
maxhops	Use to restrict the forwarded times of one BPDU. The default value is 20.
hellotime	The default value is 2. This is a per-Bridge parameter in RSTP, it is existed only in STP/RSTP Mode..
forwarddelay	The maximum delay time for one BPDU to be transmitted by a bridge and received from another bridge. The default value is 15.
txholdcount	Use to restrict the numbers of BPDU transmitted in a time interval（per Hello Time）.
fbpdu	Use to decide if the Bridge will flood STP BPDU when STP functionality is disabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure STP:

```
DGS-3200-10:4#config stp maxage 10 maxhops 4 forwarddelay 15
Command: config stp maxage 10 maxhops 4 forwarddelay 15

Success.

DGS-3200-10:4#
```

27-14 config stp ports

Purpose

To configure STP command port parameters on the switch.

Format

config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false | auto] | state [enable | disable] | restricted_role [true | false] | restricted_tcn [true | false] | fbpdu [enable | disable]}

Description

This command is used to configure STP command port parameters on the switch.

Parameters

Parameters	Description
portlist	One of the CLI Value Types, restricts the input value and format of the ports.
externalCost	The path cost between the MST regions from the transmitting Bridge to the CIST Root Bridge. It is only used at CIST level.
hellotime	The default value is 2 . This is a per-Bridge parameter in RSTP, but it becomes a per-Port parameter in MSTP.
migrate	Operation of management in order to specify the port to send MSTP BPDU for a delay time.
edge	Decide if this port is connected to a LAN or a bridged LAN. In auto mode, the bridge will delay for a period to become edge port if no bridge BPUD is received.
p2p	Decide if this port is in Full-Duplex or Half-Duplex mode.
state	Decide if this port supports the STP functionality.
restricted_role	Decide if this port is to be selected as Root Port or not. *true* - Decide that this port is not to be selected as Root Port. *false* - Decide that this port is to be selected as Root Port. This is the default.
restricted_tcn	Decide if this port is to propagate a topology change or not. *true* - Specify not to propagate a topology change. *false* - Specify to propagate a topology change. This is the default.
fbpdu	Decide if this port will flood STP BPDU when STP functionality is disabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To config STP ports:

```
DGS-3200-10:4#config stp ports 1 externalCost auto
Command: config stp ports 1 externalCost auto

Success.

DGS-3200-10:4#
```

27-15 config stp mst_ports

Purpose

To configure the MSTI STP port status for a port list on the switch.

Format

config stp mst_ports <portlist> instance_id <value 0-15> { internalCost [auto | <value 1-200000000>] | priority <value 0-240> }

Description

This command is used to configure the MSTI STP port status for a port list on the switch.

Parameters

Parameters	Description
mst_ports	Distinguished from the parameters of ports only at the CIST level.
portlist	One of the CLI value types, restricts the input value and format of the ports.
instance_id	Instance = 0 represents CIST, Instance from 1 to 15 represents MSTI 1 to MSTI 15 .
internalCost	The port path cost used in MSTP.
priority	The port priority.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure STP MST ports:

```
DGS-3200-10:4#config stp mst_ports 1 instance_id 0 internalCost auto
Command: config stp mst_ports 1 instance_id 0 internalCost auto

Success.

DGS-3200-10:4#
```

27-16 config stp trap

Purpose

To configure the sending state for STP traps.

Format

config stp trap { new_root [enable | disable] topo_change [enable |disable]}

Description

This command is used to configure the sending state for STP traps..

Parameters

Parameters	Description
new_root	Enable or disable the sending of new root traps. The default state is enabled.
topo_change	Enable or disable the sending of topology change traps. The default state is enabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the sending state for STP traps:

```
DGS-3200-10:4#config stp trap new_root disable
Command: config stp trap new_root disable

Success.

DGS-3200-10:4#
```

28 FDB Command List

create fdb <vlan_name 32> <macaddr> [port <port> | drop]
create fdb vlanid <vidlist> <macaddr> [port <port> | drop]
create multicast_fdb <vlan_name 32> <macaddr>
config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time <sec 10-875>
config multicast vlan_filtering_mode [vlanid <vidlist>|vlan <vlan_name 32>|all] [forward_unregistered_groups|filter_unregistered_groups]
delete fdb<vlan_name 32> <macaddr>
clear fdb [vlan <vlan_name 32> | port <port> | all]
show multicast_fdb { vlan <vlan_name 32> | mac_address <macaddr> }
show fdb {[port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time | security]}
show multicast vlan_filtering_mode {vlanid <vidlist>|vlan <vlan_name 32>}

28-1 create fdb

Purpose

To create a static entry to the unicast MAC address forwarding table (database).

Format

create fdb <vlan_name 32> <macaddr> [port <port> | drop]

Description

This command is used to make an entry into the switch's unicast MAC address forwarding database.

Parameters

Parameters	Description
<vlan_name 32>	Specify a VLAN name associated with a MAC address.
macaddr	The MAC address to be added to the static forwarding table.
port	The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.
drop	Specify to have the Switch to drop traffic.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an unicast MAC forwarding:

```
DGS-3200-10:4#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DGS-3200-10:4#
```

28-2 create fdb vlanid

Purpose

To create an entry into the switch's unicast MAC address forwarding database using the VLAN ID.

Format

create fdb vlanid <vidlist> <macaddr> [port <port> | drop]

Description

This command is used to create an entry into the switch's unicast MAC address forwarding database using the VLAN ID.

Parameters

Parameters	Description
<vidlist>	Specify the VLAN ID.
<macaddr>	Specify the MAC address to be added to the static forwarding table.
port	Specify the port number corresponding to the MAC destination address.
drop	Specify to have the Switch drop traffic.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an unicast MAC forwarding:

```
DGS-3200-10:4# create fdb vlanid 1 00-11-22-33-44-55 port 1
Command: create fdb vlanid 1 00-11-22-33-44-55 port 1

Success.

DGS-3200-10:4#
```

28-3 create multicast_fdb

Purpose

To create a static entry to the multicast MAC address forwarding table (database).

Format

create multicast_fdb <vlan_name 32> <macaddr>

Description

This command is used to make an entry into the switch's multicast MAC address forwarding database.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
macaddr	The multicast MAC address to be added to the static forwarding table.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create multicast MAC forwarding:

```
DGS-3200-10:4# create multicast_fdb default 01-00-5E-00-00-00
Command: create multicast_fdb default 01-00-5E-00-00-00

Success.

DGS-3200-10:4#
```

28-4 config multicast_fdb

Purpose

To configure the switch's multicast MAC address forwarding database.

Format

config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>

Description

This command is used to configure the multicast MAC address forwarding table.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum name length is 32.
macaddr	The MAC address that will be added or deleted to the forwarding table.
portlist	Specifiy a range of ports to be configured.
add	Specify to add a range of ports.
delete	Specify to delete a range of ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add multicast MAC forwarding:

```
DGS-3200-10:4# config multicast_fdb default 01-00-5E-00-00-00 add 1-5
Command: config multicast_fdb default 01-00-5E-00-00-00 add 1-5

Success.

DGS-3200-10:4#
```

28-5 config fdb aging_time

Purpose

To configure the switch's MAC address aging time.

Format

config fdb aging_time <sec 10-875>

Description

This command is used to set the age-out timer for the switch's dynamic unicast MAC address forwarding tables.

Parameters

Parameters	Description
aging_time	Specify the time, in seconds, that a dynamically learned MAC address will remain in the switch's MAC address forwarding table, without being accessed, before being dropped from the database. The range of the value is 10 to 875. The default value is 300.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure MAC address aging time:

```
DGS-3200-10:4#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3200-10:4#
```

28-6 config multicast vlan_filtering_mode

Purpose

To configure the multicast packet filtering mode for VLANs.

Format

config multicast vlan_filtering_mode [vlanid <vidlist>|vlan <vlan_name 32> |all]
[forward_unregistered_groups|filter_unregistered_groups]

Description

This command is used to configure the multicast packet filtering mode for VLANs.

Parameters

Parameters	Description
vlanid	Specify a VLAN ID list to set.
vlan	Spcify a VLAN name to set.
all	Specify all VLANs to set.
forward_unregistered_groups	The filtering mode can be **forward_unregistered_groups**, or **filter_unregistered_groups**.
filter_unregistered_groups	

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the multicast packet filtering mode for all VLAN:

```
DGS-3200-10:4#config multicast vlan_filtering_mode all forward_unregistered_groups
Command: config multicast port filtering_mode all forward_unregistered_groups

Success.

DGS-3200-10:4#
```

28-7 delete fdb

Purpose

To delete an entry to the switch's forwarding database.

Format

delete fdb <vlan_name 32> <macaddr>

Description

This command is used to delete a permanent FDB entry.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
macaddr	The MAC address to be deleted from the static forwarding table.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a permanent FDB entry:

```
DGS-3200-10:4#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3200-10:4#
```

28-8 clear fdb

Purpose

To clear the switch's forwarding database of all dynamically learned MAC addresses.

Format

clear fdb [vlan <vlan_name 32> | port <port> | all]

Description

This command is used to clear the switch's forwarding database of all dynamically learned MAC addresses.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
port	The port number corresponding to the dynamically learned MAC address.
all	Specify to clear all the switch's FDB of dynamically learned MAC addresses.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear all FDB dynamic entries:

```
DGS-3200-10:4#clear fdb all
Command: clear fdb all

Success.

DGS-3200-10:4#
```

28-9 show multicast_fdb

Purpose

To display the contents of the switch's multicast forwarding database.

Format

show multicast_fdb { vlan <vlan_name 32> | mac_address <macaddr> }

Description

This command is used to display the contents of the switch's multicast forwarding database. If no parameter is specified, all multicast fdb entries will be displayed.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN on which the MAC address resides. The maximum length is 32.
macaddr	Specify a MAC address, for which FDB entries will be displayed.

Restrictions

None.

Examples

To display multicast MAC address table:

```
DGS-3200-10:4#show multicast_fdb
Command: show multicast_fdb

VLAN Name     : default
MAC Address   : 01-00-5E-00-00-00
Egress Ports  : 1-5,26
Mode          : Static

Total Entries : 1

DGS-3200-10:4#
```

28-10 show fdb

Purpose

To display the current unicast MAC address forwarding database.

Format

show fdb {[port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time | security]}

Description

This command is used to display the current unicast MAC address forwarding database. If no parameter is specified, the system will display the unicast address table.

Parameters

Parameters	Description
port	Specify to display the entries for one port.
vlan	Specify to display the entries for a specific VLAN.

mac_address	Specify to display the entries for a specific MAC address.
static	Specify to display all permanent entries.
aging_time	Specify to display the unicast MAC address aging time.
security	Specify to display the security settings.

Restrictions

None.

Examples

To display unicast MAC address table:

```
DGS-3200-10:4#show fdb
Command: show fdb

Unicast MAC Address Ageing Time = 300

VID    VLAN Name          MAC Address         Port     Type
----   ----------------   -----------------   ------   ----------------
1      default            00-00-00-00-01-02    5      Permanent
1      default            00-01-02-03-04-00   CPU      Self

Total Entries : 2

DGS-3200-10:4#
```

28-11 show multicast vlan_filtering_mode

Purpose

To show the multicast packet filtering mode for VLANs.

Format

show multicast vlan_filtering_mode {vlanid <vidlist>|vlan <vlan_name 32>}

Description

This command is used to display the multicast packet filtering mode for VLANs. If no parameter is specified, the system will display all VLANs in multicast packet filtering mode.

Parameters

Parameters	Description
vidlist	Display the entries by VLAN ID list.
vlan_name 32	Display the entries for a specific VLAN.

Restrictions

None.

Examples

To show multicast filtering mode for VLANs:

```
DGS-3200-10:4#show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name                            Multicast Filter Mode
---------------------------------------    ------------------------------
1   /default                                forward_unregistered_groups
2   /123                                    forward_unregistered_groups

DGS-3200-10:4#
```

29 MAC Notification Command List

enable mac_notification
disable mac_notification
config mac_notification{interval <int 1-2147483647>|historysize <int 1-500>}
config mac_notification ports [<portlist>|all] [enable|disable]
show mac_notification
show mac_notification ports{<portlist>}

29-1 enable mac_notification

Purpose

To enable global MAC address table notification on the switch.

Format

enable mac_notification

Description

This command is used to enable global MAC address table notification on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the MAC notification function:

```
DGS-3200-10:4#enable mac_notification
Command: enable mac_notification

Success.

DGS-3200-10:4#
```

29-2 disable mac_notification

Purpose

To disable global MAC address table notification on the switch.

Format

disable mac_notification

Description

This command is used to disable global MAC address table notification on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the MAC notification function:

```
DGS-3200-10:4#disable mac_notification
Command: disable mac_notification

Success.

DGS-3200-10:4#
```

29-3 config mac_notification

Purpose

To configure the switch's MAC address table notification global settings.

Format

config mac_notification{interval <int 1-2147483647>|historysize <int 1-500>}

Description

This command is used to configure the switch's MAC address table notification global settings.

Parameters

Parameters	Description
interval	The time in seconds between notifications.
historysize	This is the maximum number of entries listed in the history log used for notification. Up to 500 entries can be specified.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the switch's MAC address table notification global settings:

```
DGS-3200-10:4#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3200-10:4#
```

29-4 config mac_notification ports

Purpose

To configure the port's MAC address table notification status settings.

Format

config mac_notification ports [<portlist>|all] [enable(3)|disable(2)]

Description

This command is used to configure the port's MAC address table notification status settings.

Parameters

Parameters	Description
portlist	Specifiy a range of ports to be configured.
all	To set all ports in the system, use the **all** parameter.
enable	Enable the port's MAC address table notification.
disable	Disable the port's MAC address table notification.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable MAC address table notification for Port 7:

```
DGS-3200-10:4#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3200-10:4#
```

29-5 show mac_notification

Purpose

To display the switch's MAC address table notification global settings.

Format

show mac_notification

Description

This command is used to display the switch's MAC address table notification global settings.

Parameters

None.

Restrictions

None.

Examples

To show the switch's MAC address table notification global settings:

```
DGS-3200-10:4#show mac_notification
Command: show mac_notification

Global MAC Notification Settings

State            : Enabled
Interval         : 1
History Size     : 500

DGS-3200-10:4#
```

29-6 show mac_notification ports

Purpose

To display the port's MAC address table notification status settings.

Format

show mac_notification ports{<portlist>}

Description

This command is used to display the port's MAC address table notification status settings.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.

Restrictions

None.

Examples

To display the MAC address table notification status settings of all ports:

```
DGS-3200-10:4#show mac_notification ports 1-10
Command: show mac_notification ports 1-10

Port #  MAC Address Table Notification State
------  ------------------------------------
1                   Disabled
2                   Disabled
3                   Disabled
4                   Disabled
5                   Disabled
6                   Disabled
7                   Disabled
8                   Disabled
9                   Disabled
10                  Disabled

DGS-3200-10:4#
```

30 Mirror Command List

config mirror port <port> [add|delete] source ports <portlist> [rx | tx | both]
enable mirror
disable mirror
show mirror

30-1 config mirror port

Purpose

To configure a mirror port – a source port pair on the switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe can then be attached to study the traffic crossing the source port in a completely unobtrusive manner.

Format

config mirror port <port> [add \|delete] source ports <portlist> [rx\|tx\|both]

Description

This command is used to allow a range of ports to have all of their traffic also sent to a designated port – where a network sniffer or other device can monitor the network traffic. In addition, you can specify that only traffic received by or sent by or both is mirrored to the target port.

Parameters

Parameters	Description
port	The port that will receive the packets duplicated at the mirror port.
add	The mirror entry to be added.
delete	The mirror entry to be deleted.
portlist	The port that will be mirrored. All packets entering and leaving the source port can be duplicated in the mirror port.
rx	Allow the mirroring of only packets received (flowing into) the port or ports in the port list.
tx	Allow the mirroring of only packets sent (flowing out of) the port or ports in the port list.
both	Mirrors all the packets received or sent by the port or ports in the port list.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add mirroring ports:

```
DGS-3200-10:4#config mirror port 6 add source ports 1-5 both
Command: config mirror port 6 add source ports 1-5 both

Success.

DGS-3200-10:4#
```

30-2 enable mirror

Purpose

To enable a previously entered port mirroring configuration.

Format

enable mirror

Description

This command is used to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

Note: If the target port hasn't been set, **enable mirror** will not be allowed.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable mirroring configurations:

```
DGS-3200-10:4#enable mirror
Command: enable mirror

Success.

DGS-3200-10:4#
```

30-3 disable mirror

Purpose

To disable a previously entered port mirroring configuration.

Format

disable mirror

Description

This command, combined with the **enable mirror** command above, allows you to enter a port mirroring configuration into the switch, and then turn the port mirroring on and off without having to modify the port mirroring configuration.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable mirroring configurations:

```
DGS-3200-10:4#disable mirror
Command: disable mirror

Success.

DGS-3200-10:4#
```

30-4 show mirror

Purpose

To show the current port mirroring configuration on the switch.

Format

show mirror

Description

This command is used to display the current port mirroring configuration on the switch.

Parameters

None.

Restrictions

None.

Examples

To display mirroring configuration:

```
DGS-3200-10:4#show mirror
Command: show mirror

Current Settings
Mirror Status : Disabled
Target Port   : 7
Mirrored Port
            RX:
            TX: 1-5

DGS-3200-10:4#
```

31 VLAN Command List

create vlan <vlan_name 32 > tag <vlanid 2-4094> { type [1q_vlan {advertisement} | private_vlan] }
create vlan vlanid <vidlist> { type [1q_vlan | private_vlan] { advertisement } }
delete vlan <vlan_name>
delete vlan vlanid <vlanid_list>
config vlan < vlan_name > { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] }
config vlan vlanid <vidlist> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]| name <vlan_name>}
config vlan <vlan_name> delete <portlist>
config vlan vlanid <vlanid_list> delete <portlist>
config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] |acceptable_frame[tagged_only | admit_all] pvid<vlanid 1-4094> }
enable gvrp
disable gvrp
show vlan { <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>}
show gvrp {<portlist>}
enable pvid auto_assign
disable pvid auto_assign
show pvid auto_assign
config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove] [<vlan_name 32> | vlanid <vidlist>]
show private_vlan { [vlan_name 32> | vlanid <vidlist>] }

31-1 create vlan

Purpose

To create a VLAN on the switch.

Format

create vlan <vlan_name 32 > tag <vlanid 2-4094> { type [1q_vlan {advertisement} | private_vlan} }
create vlan vlanid <vidlist> { type [1q_vlan | private_vlan] { advertisement }}

Description

This command is used to create a VLAN on the switch. The VLAN ID must be always specified for creating a VLAN.

Parameters

Parameters	Description
vlan_name	The name of the VLAN to be created.
vlanid	The VLAN ID of the VLAN to be created.
type	Specify the VLAN type. If nothing is specified, the created VLAN is a regular 802.1Q VLAN.
tag	The VLAN ID of the VLAN to be created. The range is from 2 to 4094.
advertisement	Specify the VLAN as being able to be advertised out.
private_vlan	Specify to create a private VLAN. Up to 24 private VLANs can be created on the switch.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a VLAN with the name “v2” and VLAN ID 2:

```
DGS-3200-10:4#create vlan v2 tag 2 type 1q_vlan advertisement
Command: create vlan v2 tag 2 type 1q_vlan advertisement

Success.

DGS-3200-10:4#
```

To create a private VLAN with the name “v3” and VLAN ID 3:

```
DGS-3200-10:4#create vlan v3 tag 3 type private_vlan
Command: create vlan v3 tag 3 type private_vlan

Success.

DGS-3200-10:4#
```

31-2 delete vlan

Purpose

To delete a previously configured VLAN on the switch.

Format

delete vlan <vlan_name>

delete vlan vlanid <vlanid_list>

Description

These commands are used to delete a previously configured VLAN on the switch. However, if an 802.1Q VLAN is added as a private VLAN, it can't be deleted.

Parameters

Parameters	Description
vlan_name	The VLAN name of the VLAN to be deleted.
vlan vlanid	The VLAN ID of the VLAN to be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To remove a VLAN v1:

```
DGS-3200-10:4#delete vlan v1
Command: delete vlan v1

Success.

DGS-3200-10:4#
```

31-3 config vlan add ports

Purpose

To add additional ports to a previously configured VLAN.

Format

config vlan <vlan_name 32> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}

config vlan vlanid <vidlist> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable] | name <vlan_name 32>}

Description

This command is used to add ports to the port list of a previously configured VLAN. You can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN you want to add ports to.
vlan vlanid	The VLAN ID of the VLAN you want to add ports to.

tagged	Specify the additional ports as tagged.
untagged	Specify the additional ports as untagged.
forbidden	Specify the additional ports as forbidden.
portlist	A range of ports to add to the VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add 4 through 8 as tagged ports to the VLAN v1:

```
DGS-3200-10:4#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DGS-3200-10:4#
```

31-4 config vlan delete ports

Purpose

To delete one or more ports from a previously configured VLAN.

Format

config vlan <vlan_name 32> delete <portlist>

config vlan vlanid <vlanid_list> delete <portlist>

Description

This command is used to delete one or more ports from a previously configured VLAN.

Parameters

Parameters	Description
vlan_name 32	The name of the VLAN you want to delete ports from.
vlan vlanid	The VLAN ID of the VLAN you want to delete ports from.
portlist	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete ports 4 through 8 from VLAN v1:

```
DGS-3200-10:4#config vlan v1 delete 4-8
Command: config vlan v1 delete 4-8

Success.

DGS-3200-10:4#
```

31-5 config vlan advertisement

Purpose

To enable or disable the VLAN advertisement.

Format

config vlan vlanid <vidlist> advertisement [enable | disable]

Description

This command is used to enable or disable the VLAN advertisement.

Parameters

Parameters	Description
vlan vlanid	The VLAN ID of the VLAN on which you want to configure.
advertisement	Join GVRP or not. If not, the VLAN can't join dynamically

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the VLAN default advertisement:

```
DGS-3200-10:4#config vlan default advertisement enable
Command: config vlan default advertisement enable

Success.

DGS-3200-10:4#
```

31-6 config gvrp

Purpose

To set the ingress checking status and the sending and receiving of GVRP information.

Format

config gvrp [<portlist> | all] {state [enable | disable] | ingress_checking [enable | disable] | acceptable_frame [tagged_only | admit_all] pvid<vlanid 1-4094> }

Description

This command is used to set the ingress checking status and the sending and receiving of GVRP information.

Parameter

Parameters	Description	
portlist	A range of ports for which you want ingress checking. The beginning and end of the port list range are separated by a dash.	
state	Enable or disable GVRP for the ports specified in the port list.	
ingress_checking	Enable or disable ingress checking for the specified portlist.	
acceptable_frame	The type of frame will be accepted by the port.	
	tagged_only	Only tagged frame will be received.
	admit_all	Both tagged and untagged will be accepted.
pvid	Specify the default VLAN will associated with the port.	

Restrictions

Only Administrator-level users can issue this command.

Example

To set the ingress checking status and send and receive GVRP information:

```
DGS-3200-10:4#config gvrp 5 state enable ingress_checking enable acceptable_
frame tagged_only pvid 2
Command: config gvrp 5 state enable ingress_checking enable acceptable_frame
tagged_only pvid 2

Success

DGS-3200-10:4#
```

31-7 enable gvrp

Purpose

To enable the Generic VLAN Registration Protocol (GVRP).

Format

enable gvrp

Description

This command is used to enable the Generic VLAN Registration Protocol (GVRP). The default setting is disabled.

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3200-10:4#enable gvrp
Command: enable gvrp

Success.

DGS-3200-10:4#
```

31-8 disable gvrp

Purpose

To disable Generic VLAN Registration Protocol (GVRP).

Format

disable gvrp

Description

This command is used to disable Generic VLAN Registration Protocol (GVRP).

Parameter

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable Generic VLAN Registration Protocol (GVRP) :

```
DGS-3200-10:4#disable gvrp
```

```
Command: disable gvrp

Success.

DGS-3200-10:4#
```

31-9 show vlan

Purpose

To display the VLAN information including of parameters setting and operational value.

Format

show vlan { <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>}

Description

This command is used to display summary information about each VLAN, which includes: VLAN ID, VLAN Name, Tagged/Untagged/Forbidden status for each port, and Member/Non-member status for each port.

Parameters

Parameters	Description
vlan_name	The name of the VLAN to be displayed.
vlanid	The VLAN ID number to be displayed.
ports	A range of ports for which you want to display VLAN. The beginning and end of the port list range are separated by a dash.

Restrictions

None.

Examples

To display VLAN settings:

```
DGS-3200-10:4#show vlan
Command: show vlan

VLAN Trunk State         : Disabled
VLAN Trunk Member Ports :



VID              : 1               VLAN Name      : default
VLAN Type        : Static          Advertisement : Enabled
Member Ports     : 1-7
Static Ports     : 1-6
Current Tagged Ports:
Current Untagged Ports  : 1-7
Static Tagged Ports:
Static Untagged Ports   : 1-6
Forbidden Ports :

Total Static VLAN Entries: 1
Total GVRP VLAN Entries: 0

DGS-3200-10:4#
```

To display VLAN port settings:

```
DGS-3200-10:4#show vlan ports 1-2
Command: show vlan ports 1-2

Port       VID    Untagged   Tagged   Dynamic  Forbidden
------      -----  --------   ------   -------  ---------
 1          1        X          -         -        -
 2          1        X          -         -        -

DGS-3200-10:4#
```

31-10 show gvrp

Purpose

To display the GVRP status for a port list on the switch.

Format

show gvrp {<portlist>}

Description

This command is used to display the GVRP status for a port list on the switch. If no parameter is specified, the system will display GVRP information for all ports.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Example

To display the 802.1q port setting for ports 1 through 6:

```
DGS-3200-10:4#show gvrp 1-6
Command: show gvrp 1-6

Global GVRP : Enabled

Port    PVID  GVRP      Ingress Checking  Acceptable Frame Type
------  ----  --------  ----------------  --------------------------
1       2     Enabled   Enabled           Only VLAN-tagged frames
2       2     Enabled   Enabled           Only VLAN-tagged frames
3       2     Enabled   Enabled           Only VLAN-tagged frames
4       2     Enabled   Enabled           Only VLAN-tagged frames
5       2     Enabled   Enabled           Only VLAN-tagged frames
6       1     Disabled  Enabled           All Frames

Total Entries : 6

DGS-3200-10:4#
```

31-11 enable pvid auto_assign

Purpose

To enable auto assignment of PVID.

Format

enable pvid auto_assign

Description

This command is used to enable the auto-assignment of PVID. If “auto-assign PVID” is disabled, PVID can only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. If “auto-assign PVID” is enabled, PVID can be changed by PVID or VLAN configuration. When a user configures a port to VLAN X’s untagged membership, this port’s PVID will be updated with VLAN X. PVID is updated with the last item of the VLAN list. When a user removes a port from the untagged membership of the PVID’s VLAN, the port’s PVID will be assigned with “default VLAN”. The default setting is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable the auto-assign PVID:

```
DGS-3200-10::4#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3200-10::4#
```

31-12 disable pvid auto_assign

Purpose

To disable auto assignment of PVID.

Format

disable pvid auto_assign

Description

This command is used to disable auto assignment of PVID.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the auto-assign PVID:

```
DGS-3200-10::4#disable pvid auto_assign
Command: disable pvid auto_assign

Success.

DGS-3200-10::4#
```

31-13 show pvid auto_assign

Purpose

To display the PVID auto-assignment state.

Format

show pvid auto_assign

Description

This command is used to display the PVID auto-assign state.

Parameters

None.

Restrictions

You must have user-level privileges.

Example

To display the PVID auto-assignment state:

```
DGS-3200-10::4#show pvid auto_assign

PVID Auto-assignment: Enabled.

DGS-3200-10::4#
```

31-14 config private_vlan

Purpose

To add or remove secondary VLANs to/from a private VLAN.

Format

config private_vlan [<vlan_name 32> | vid <vlanid 1-4094>] [add [isolated | community] | remove]

[<vlan_name 32> | vlanid <vidlist>]

Description

This command is used to add or remove secondary VLANs to/from a private VLAN.

A private VLAN is made up of a primary VLAN, up to one isolated VLAN, and a number of community VLANs. The private VLAN ID is represented by the VLAN ID of the primary VLAN.

The purpose of a primary VLAN is to transfer unidirectional traffic downstream from promiscuous ports to isolated and community host ports and to other promiscuous ports.

The Switch supports two types of secondary VLANs, isolated and community VLANs.

The primary VLAN member port cannot be a secondary VLAN member at the same time and vice-versa.

A secondary VLAN can only contain untagged member ports.

A port cannot be a member of more then one secondary VLAN at the same time.

Parameters

Parameters	Description
vlan_name	The name of the private VLAN.
vlanid	The VLAN ID of the private VLAN.
isolated	Specifies that the secondary VLAN will be an isolated VLAN. An isolated VLAN is a secondary VLAN whose distinct characteristic is that all hosts connected to its ports are isolated at Layer 2. The primary advantage of an isolated VLAN is that it allows a Private VLAN to only use two VLAN identifiers to provide port isolation and serve any number of end users. A Private VLAN can only support one isolated VLAN.
community	Specifies that the secondary VLAN will be a community VLAN. A community VLAN is a secondary VLAN that is associated with a group of ports that connects to a certain "community" of end devices with mutual trust relationships. There can be multiple distinct community VLANs in a private VLAN domain.
vidlist	A range of secondary VLANs to add or remove to the private VLAN.

Restrictions

You must have user-level privileges.

Example

To associate a secondary VLAN to private VLAN p1:

```
DGS-3200-10:4#config private_vlan p1 add community vlanid 2-5
Command: config private_vlan p1 add community vlanid 2-5

Success.

DGS-3200-10:4#
```

31-15 show private_vlan

Purpose

To display the private VLAN information.

Format

show private_vlan {vlan <vlan_name 32> | vlanid <vidlist>}

Description

This command is used to display private VLAN information for the switch.

Parameters

Parameters	Description
vlan_name	The name of the private VLAN or its secondary VLAN.
vlanid	The VLAN ID of the private VLAN or its secondary VLAN.

Restrictions

None.

Example

To display private VLAN settings:

```
DGS-3200-10:4# show private_vlan
Command: show private_vlan
Private VLAN 100
------------------
    Promiscuous Ports: 1
    Trunk Ports      : 2
    Isolated Ports   : 3-5           Isolated VLAN : 20
Community Ports  : 6-8           Community VLAN: 30
    Community Ports  : 9-10          Community VLAN: 40

Private VLAN 200
------------------
    Promiscuous Ports:
    Trunk Ports      :

 Total Entries: 2
DGS-3200-10:4#
```

32 Voice VLAN Command List

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]
disable voice_vlan
config voice_vlan priority <int 0-7>
config voice_vlan oui [add | delete] <macaddr> < macmask> {description <desc 32>}
config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto {[tag | untag]} | manual]]
config voice_vlan log state [enable|disable]
config voice_vlan aging_time <min 1-65535>
show voice_vlan
show voice_vlan oui
show voice_vlan ports {<portlist>}
show voice_vlan voice_device { ports <portlist>}
show voice_vlan lldp_med voice_device

32-1 enable voice_vlan

Purpose

To enable the global voice VLAN function on the Switch.

Format

enable voice_vlan [<vlan_name 32> | vlanid <vlanid 1-4094>]

Description

This command is used to enable the global voice VLAN function on the Switch. To enable the voice VLAN, the voice VLAN must be also assigned. At the same time, the VLAN must be an existing static 802.1Q VLAN. To change the voice VLAN, the user must disable the voice VLAN function, and re-issue this command. By default, the global voice VLAN state is disabled.

Parameters

Parameters	Description
<vlan_name 32>	Specify the name of the voice VLAN. The maximum length is 32 characters. The name must be an existing static VLAN name.
vlanid	Specify the VLAN ID of the voice VLAN. The ID must be an existing static VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable voice VLAN named v2:

```
DGS-3200-10:4# enable voice_vlan v2
Command: enable voice_vlan v2

Success.

DGS-3200-10:4#
```

32-2 disable voice_vlan

Purpose

To disable the voice VLAN function on the Switch.

Format

disable voice_vlan

Description

This command is used to disable the voice VLAN function on the Switch. When the voice VLAN function is disabled, the voice VLAN will become unassigned.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable voice VLAN:

```
DGS-3200-10:4# disable voice_vlan
Command: disable voice_vlan

Success.

DGS-3200-10:4#
```

32-3 config voice_vlan priority

Purpose

To configure voice VLAN priority.

Format

config voice_vlan priority <int 0-7>

Description

This command is used to configure voice VLAN priority. The voice VLAN priority will be the priority associated with the voice VLAN traffic to distinguish the QoS of the voice traffic from data traffic.

Parameters

Parameters	Description
<int 0-7>	Specify the priority of the voice VLAN. The range is 0 to 7. The default priority is 5.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the priority of the voice VLAN to be 6:

```
DGS-3200-10:4# config voice_vlan priority 6
Command: config voice_vlan priority 6

Success.

DGS-3200-10:4#
```

32-4 config voice_vlan oui

Purpose

To configure the user-defined voice traffic's OUI.

Format

config voice_vlan oui [add | delete] <macaddr> < macmask> {description <desc 32>}

Description

This command is used to configure the user-defined voice traffic's OUI. The OUI is used to identify the voice traffic. There are a number of pre-defined OUIs. The user can further define the user-defined OUIs if needed. The user-defined OUI cannot be the same as the pre-defined OUI. The following are the pre-defined voice traffic's OUI:

OUI	Vendor	Mnemonic Name
00:E0:BB	3COM	3com
00:03:6B	Cisco	cisco
00:E0:75	Veritel	veritel
00:D0:1E	Pingtel	pingtel
00:01:E3	Siemens	siemens
00:60:B9	NEC/ Philips	nec&philips
00:0F:E2	Huawei-3COM	huawei&3com
00:09:6E	Avaya	avaya

Parameters

Parameters	Description
add	Specify to add a user-defined OUI of Voice device vendor.
delete	Specify to delete a user-defined OUI of Voice device vendor.
<macaddr>	Specify a user-defined OUI MAC address.
<macmask>	Specify a user-defined OUI MAC address mask.
description	Specify a description for the user-defined OUI. The maximum length is 32 characters.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a user-defined OUI of a voice device:

```
DGS-3200-10:4# config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00
Command: config voice_vlan oui add 00-0A-0B-00-00-00 FF-FF-FF-00-00-00

Success.

DGS-3200-10:4#
```

32-5 config voice_vlan ports

Purpose

To enable or disable the voice VLAN function on ports or mode per port.

Format

config voice_vlan ports [<portlist> | all] [state [enable | disable] | mode [auto {[tag | untag]} | manual]]

Description

This command is used to enable or disable the voice VLAN function on ports or mode per port.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be configured.
all	Specify all ports to be configured.
state	Specify to enable or disable the voice VLAN function state on ports. The default state is disabled.
mode	Specify the voice VLAN mode. The default mode is auto. **auto** - When the mode is auto, the port may become the voice VLAN member port by auto-learning. If the MAC address of the received packet matches the configured OUI, the port will be learned as dynamic member port. The dynamic membership will be removed via the aging out mechanism. **tag** - Specify the port to join the voice VLAN as a tagged member. **untag** - Specify the port to join the voice VLAN as an untagged member. • When the port is working in auto tagged mode, and learns about a voice device through the device's OUI, it will join the voice VLAN as a tagged member automatically. When the voice device sends voice VLAN tagged packets, the Switch will change its priority. When the voice device sends untagged packets, it will forward them to port's PVID VLAN. • When the port is working in auto untagged mode, and the port captures a voice device through the device's OUI, it will join the voice VLAN as an untagged member automatically. When the voice device sends voice VLAN tagged packets, the Switch will change its priority. Should the voice device send untagged packets, the Switch will assign priority and add the voice VLAN ID into these packets. • When the switch receives LLDP-MED packets, it checks the VLAN ID, tagged flag and priority flag.The Switch should follow the tagged flag and priority setting. **manual** - When the mode is set to manual, the port needs to be manually added into or removed from the voice VLAN by 802.1Q VLAN configuration command. By default, the mode is auto untagged.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure voice VLAN ports 4 to 6 to enable:

```
DGS-3200-10:4# config voice_vlan ports 4-6 state enable
Command: config voice_vlan ports 4-6 state enable

Success.

DGS-3200-10:4#
```

32-6 config voice_vlan log state

Purpose

To configure the voice VLAN log state.

Format

config voice_vlan log state [enable|disable]

Description

This command is used to configure the voice VLAN log state.

Parameters

Parameters	Description
enable	Specify to enable the voice VLAN log state.
disable	Specify to disable the voice VLAN log state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the voice VLAN log state:

```
DGS-3200-10:4# config voice_vlan log state enable
Command: config voice_vlan log state enable

Success.

DGS-3200-10:4#
```

32-7 config voice_vlan aging_time

Purpose

To set the aging time of the Voice VLAN.

Format

config voice_vlan aging_time <min 1-65535>

Description

This command is used to set the aging time of the Voice VLAN. The aging time is used to remove a port from the Voice VLAN if the port is an automatic Voice VLAN member. The Voice VLAN aging timer will start when the last voice device stops sending traffic and the MAC address of this voice device is timed out. The port will be removed from the Voice VLAN after it expires. When the voice traffic resumes during the aging time, the aging timer will reset and stop.

Parameters

Parameters	Description
<min 1-65535>	Specify the aging time between 1 and 65535 minutes. The default value is 720 minutes.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the aging time of the Voice VLAN to 60 minutes:

```
DGS-3200-10:4# config voice_vlan aging_time 60
Command: config voice_vlan aging_time 60

Success.

DGS-3200-10:4#
```

32-8 show voice_vlan

Purpose

To display voice VLAN global information.

Format

show voice_vlan

Description

This command is used to display voice VLAN global information.

Parameters

None.

Restrictions

None.

Examples

To display voice VLAN information:

```
DGS-3200-10:4# show voice_vlan
Command: show voice_vlan

Voice VLAN State   : Disabled
Voice VLAN         : Unassigned
Priority           : 5
Aging Time         : 720 minutes
Log State          : Enabled

DGS-3200-10:4#
```

32-9 show voice_vlan oui

Purpose

To display the OUI information for voice VLAN.

Format

show voice_vlan oui

Description

This command is used to display the OUI information for voice VLAN.

Parameters

None.

Restrictions

None.

Examples

To display voice VLAN OUI:

```
DGS-3200-10:4# show voice_vlan oui
Command: show voice_vlan oui
```

```
OUI Address         Mask              Description
------------------  ----------------  --------------
00-01-E3-00-00-00   FF-FF-FF-00-00-00  Siemens
00-03-6B-00-00-00   FF-FF-FF-00-00-00  Cisco
00-09-6E-00-00-00   FF-FF-FF-00-00-00  Avaya
00-0F-E2-00-00-00   FF-FF-FF-00-00-00  Huawei&3COM
00-60-B9-00-00-00   FF-FF-FF-00-00-00  NEC&Phillips
00-D0-1E-00-00-00   FF-FF-FF-00-00-00  Pingtel
00-E0-75-00-00-00   FF-FF-FF-00-00-00  Veritel
00-E0-BB-00-00-00   FF-FF-FF-00-00-00  3COM

Total Entries: 8

DGS-3200-10:4#
```

32-10 show voice_vlan ports

Purpose

To display port voice VLAN information.

Format

show voice_vlan ports {<portlist>}

Description

This command is used to display port voice VLAN information.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display voice VLAN ports 1 to 3:

```
DGS-3200-10:4# show voice_vlan ports 1-3
Command: show voice_vlan ports 1-3

Ports  Status     Mode
-----  ---------  --------
 1     Disabled   Auto
```

```
2     Disabled   Auto
3     Disabled   Auto


DGS-3200-10:4#
```

32-11 show voice_vlan voice_device

Purpose

To show voice devices that are connected to the ports.

Format

show voice_vlan voice_device { ports <portlist>}

Description

This command is used to show voice devices that are connected to the ports. The start time is the time when the device is detected on this port and the activate time is the latest time when the device sends the traffic.

Parameters

Parameters	Description
ports	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display voice VLAN device ports 1 to 2:

```
DGS-3200-10:4# show voice_vlan voice_device ports 1-2
Command: show voice_vlan voice_device ports 1-2


Ports  Voice Device      Start Time      Last Active Time
-----  ----------------  ---------------  -----------------


Total Entries : 0


DGS-3200-10:4#
```

32-12 show voice_vlan lldp_med voice_device

Purpose

To show the voice devices being discovered by the LLDP-MED.

Format

show voice_vlan lldp_med voice_device

Description

This command is used to show the voice devices being discovered by the LLDP-MED. The voice device output includes the following information:

- Index: a local index used to identify the voice device
- Local port: indicates the switch port on which voice devices are captured.
- Chassis ID subtype: chassis ID subtype of the voice device
- Chassis ID: chassis ID of the voice device
- Port ID subtype: port ID subtype of the voice device
- Port ID: port ID of the voice device
- Create Time: the time the voice device is captured
- Remain Time: the time to live remaining for the voice device. If the remaining time decreases to 0, the voice device will be deleted.

Parameters

None.

Restrictions

None.

Examples

To display the voice devices discovered by LLDP-MED:

```
DGS-3200-10:4# show voice_vlan lldp_med voice_device
Command: show voice_vlan lldp_med voice_device

Index                  : 1
Local Port             : 1
Chassis ID Subtype : MAC Address
Chassis ID             : 00-E0-BB-00-00-11
Port ID Subtype      : Network Address
Port ID                : 172.18.1.1
Create Time          : 10/6/2008 09:00
Remain Time          : 120 Seconds

Index                  : 2
Local Port             : 3
Chassis ID Subtype : MAC Address
Chassis ID             : 00-E0-BB-00-00-12
Port ID Subtype      : Network Address
Port ID                : 172.18.1.2
Create Time          : 10/6/2008 09:00
Remain Time          : 120 Seconds


Total Entries: 2

DGS-3200-10:4#
```

33 Protocol VLAN Command List

create dot1v_protocol_group group_id <id 1-8> {group_name <name 1-32>}
config dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>] add protocol [ethernet_2| ieee802.3_snap| ieee802.3_llc] <protocol_value>
config dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>] delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] < protocol_value>
delete dot1v_protocol_group [group_id <id 1-8> | group_name <name 1-32>| all]
show dot1v_protocol_group {group_id <id 1-8> | group_name <name 1-32>}
config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id 1-8> | group_name <name 1-32>] [vlan< vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-8>|all]]
show port dot1v {ports <portlist>}

33-1 create dot1v_protocol_group

Purpose

To create a protocol group for the protocol VLAN function.

Format

create dot1v_protocol_group group_id <id 1-8> {group_name <name 1-32>}

Description

This command is used to create a protocol group for the protocol VLAN function.

Parameters

Parameters	Description
group_id	The ID of the protocol group which is used to identify a set of protocols.
group_name	The name of the protocol group. The maximum length is 32 characters. If a group name is not specified, the group name will be automatically generated in accordance with ProtocolGroup+group_id. For example, the auto-generated name for group ID 2 is ProtocolGroup2. If the auto-generated name is in conflict with an existing group, an alternative name will be used in accordance with ProtocolGroup+**group_id**+ALT+num. The value for num starts with 1. If it is still in conflict, then subsequent number will be used instead. For example, the auto-generated name for group ID 1 is

	"ProtocolGroup1." If this name already exists, then "ProtocolGroup1ALT1" will be used instead.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a protocol group:

```
DGS-3200-10:4#create dot1v_protocol_group  group_id 4 group_name General_Group
Command: create dot1v_protocol_group group_id 4 group_name General_Group

Success。
DGS-3200-10:4#
```

33-2 config dot1v_protocol_group add protocol

Purpose

To add a protocol to a protocol group.

Format

config dot1v_protocol_group [group_id <id 1-8>| group_name <name 1-32>] add protocol [ethernet_2| ieee802.3_snap|ieee802.3_llc] < protocol_value>

Description

This command is used to add a protocol to a protocol group. The selection of a protocol can be a pre-defined protocol type or a user defined protocol.

Parameters

Parameters	Description
group_id	The ID of the protocol group which is used to identify a set of protocols.
group_name	The name of the protocol group.
protocol_value	The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

Restrictions

Only Administrator-level users can issue this command.

Example

To add a protocol IPv6 to protocol group 4:

```
DGS-3200-10:4# config dot1v_protocol_group group_id 4 add protocol ethernet_2 86dd
Command: config dot1v_protocol_group group_id 4 add protocol ethernet_2 86dd

Success.
DGS-3200-10:4#
```

33-3 config dot1v_protocol_group delete protocol

Purpose

To delete a protocol from a protocol group.

Format

config dot1v_protocol_group [group_id <id 1-8>| group_name <name 1-32>] delete protocol [ethernet_2| ieee802.3_snap| ieee802.3_llc] < protocol_value>

Description

This command is used to delete a protocol from a protocol group.

Parameters

Parameters	Description
group_id	Specify the group ID to be deleted.
group_name	The name of the protocol group.
protocol_value	The protocol value is used to identify a protocol of the frame type specified. The form of the input is 0x0 to 0xffff. Depending on the frame type, the octet string will have one of the following values: For Ethernet II, this is a 16-bit (2-octet) hex value. For example, IPv4 is 800, IPv6 is 86dd, ARP is 806, etc. For IEEE802.3 SNAP, this is this is a 16-bit (2-octet) hex value. For IEEE802.3 LLC, this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair. The first octet is for Destination Service Access Point (DSAP) and the second octet is for Source.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a protocol IPv6 from protocol group ID 4:

```
DGS-3200-10:4# config dot1v_protocol_group_group_id 4 delete protocol  ethernet_2 86dd
Command: config dot1v_protocol_group group_id 4 delete protocol  ethernet_2 86dd

Success.
DGS-3200-10:4#
```

33-4 delete dot1v_protocol_group

Purpose

To delete a protocol group.

Format

delete dot1v_protocol_group [group_id <id 1-8>| group_name <name 1-32>| all]

Description

This command is used to delete a protocol group.

Parameters

Parameters	Description
group_id	Specify the group ID to be deleted.
group_name	The name of the protocol group.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete protocol group ID 4:

```
DGS-3200-10:4# delete dot1v_protocol_group group_id 4
Command: delete dot1v_protocol_group group_id 4

Success.
DGS-3200-10:4#
```

33-5 show dot1v_protocol_group

Purpose

To display the protocols defined in a protocol group.

Format

show dot1v_protocol_group {group_id <id 1-8> | group_name <name 1-32->}

Description

This command is used to display the protocols defined in protocol groups.

Parameters

Parameters	Description
group_id	Specify the ID of the group to be displayed if a group ID is not specified, all configured protocol groups will be displayed
group_name	The name of the protocol group.

Restrictions

None.

Example

To display protocol group ID 4:

```
DGS-3200-10:4# show dot1v_protocol_group group_id 4
Command: show dot1v_protocol_group group_id 4

Protocol         Protocol              Frame Type             Protocol
Group ID        Group Name                                      Value
---------      ---------------       ------------         ------------
4              General Group          EthernetII              86dd

Success.
DGS-3200-10:4#
```

33-6 config port dot1v

Purpose

To assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured.

Format

config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id 1-8>| group_name <name 1-32>] [vlan < vlan_name 32> | vlanid <vlanid 1-4094>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-8>|all]]

Description

This command is used to assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured. This assignment can be removed by using the **delete protocol_group** option. When priority is not specified in the command, the port default priority will be the priority for those untagged packets classified by the protocol VLAN.

Parameters

Parameters	Description
portlist	Specify a range of ports to apply this command.
group_id	Group ID of the protocol group.
group_name	The name of the protocol group.
vlan	VLAN that is to be associated with this protocol group on this port.
vlan_id	Specify the VLAN ID .
priority	Specify the priority to be associated with the packet which has been classified to the specified VLAN by the protocol.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the group ID 4 on port 3 to be associated with VLAN 2:

```
DGS-3200-10:4# config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2
Command: config port dot1v ports 3 add protocol_group group_id 4 vlan VLAN2

Success.
DGS-3200-10:4#
```

33-7 show port dot1v

Purpose

To display the VLAN to be associated with untagged packets ingressed from a port based on the protocol group.

Format

show port dot1v {ports <portlist>}

Description

This command is used to display the VLAN to be associated with untagged packets ingressed from a port based on the protocol group.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed. If not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display the protocol VLAN information for ports 1 to 2:

```
DGS-3200-10:4# show port dot1v ports 1-2
Command: show port dot1v ports 1-2



Port : 1
Protocol Group ID     VLAN Name
----------------- --------------------------------
1                     default
2                     vlan_2
3                     vlan_3
4                     vlan_4

Port : 2 ,
Protocol Group ID     VLAN Name
----------------- --------------------------------
1                     vlan_2
2                     vlan_3
3                     vlan_4
4                     vlan_5

Success.
DGS-3200-10:4#
```

34 VLAN Trunking Command List

enable vlan_trunk
disable vlan_trunk
config vlan_trunk ports [<portlist>|all] state [enable|disable]
show vlan_trunk

34-1 enable vlan_trunk

Purpose

To enable the VLAN trunking function.

Format

enable vlan_trunk

Description

This command is used to enable VLAN trunking. When VLAN trunking function is enabled, the VLAN trunk ports shall be able to forward all tagged frames with any VID.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable VLAN trunking:

```
DGS-3200-10:4#enable vlan_trunk
Command: enable vlan_trunk


Success


DGS-3200-10:4#
```

34-2 disable vlan_trunk

Purpose

To disable the VLAN trunking function.

Format

disable vlan_trunk

Description

This command is used to disable VLAN trunking.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable VLAN trunking:

```
DGS-3200-10:4#disable vlan_trunk
Command: disable vlan_trunk

Success.

DGS-3200-10:4#
```

34-3 config vlan_trunk

Purpose

To configure a port as a VLAN trunking port.

Format

config vlan_trunk ports [<portlist>|all] | state [enabled|disabled]

Description

This command is used to configure a port as a VLAN trunking port. By default, none of the ports is a VLAN trunking port. A VLAN trunking port and a non-VLAN trunking port cannot be grouped as an aggregated link. To change the VLAN trunking setting for an aggregated link, the user must apply the command to the master port. However, this setting will disappear as the aggregated link is broken, and the VLAN trunking setting of the individual port will follow the original setting of the port. If the command is applied to link aggregation member port excluding the master, the command will be rejected. Ports with different VLAN configurations are not allowed to form an aggregated link. However, if they are specified as a VLAN trunking port, they are allowed to form an aggregated link.

For a VLAN trunking port, the VLANs on which the packets can be by passed will not be advertised by GVRP on this port. However, since the traffic on these VLANs is forwarded, this VLAN trunking port should participate in the MSTP instances corresponding to these VLANs.

Parameters

Parameters	Description
portlist	Specify the list of ports to be configured.
enable	Specify that the port is a VLAN trunking port.
disable	Specify that the port is not a VLAN trunking port.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure ports 1 to 5 as VLAN trunking ports:

```
DGS-3200-10:4#config vlan_trunk ports 1-5 state enable
Command: config vlan_trunk ports 1-5 state enable

Success.

DGS-3200-10:4#
```

To configure port 6 as an LA-1 member port and port 7 as an LA-2 master port:

```
DGS-3200-10:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

The link aggregation member port cannot be configured.
Fail.

DGS-3200-10:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

The link aggregation member port cannot be configured.
Fail.

DGS-3200-10:4#
```

To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port:

```
DGS-3200-10:4# config vlan_trunk ports 6-7 state enable
Command: config vlan_trunk ports 6-7 state enable

Success.

DGS-3200-10:4#
```

Ports 6 and 7 have different VLAN configurations before enabling VLAN trunking. To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port :

```
DGS-3200-10:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

The link aggregation needs to be deleted first.
Fail.
```

Ports 6 and 7 have the same VLAN configuration before enabling VLAN trunking. To configure port 6 as an LA-1 member port and port 7 as an LA-1 master port :

```
DGS-3200-10:4# config vlan_trunk ports 7 state disable
Command: config vlan_trunk ports 7 state disable

Success.

DGS-3200-10:4# config vlan_trunk ports 6-7 state disable
Command: config vlan_trunk ports 6-7 state disable

Success.

DGS-3200-10:4#
```

34-4 show vlan_trunk

Purpose

To show the VLAN trunking configuration.

Format

show vlan_trunk

Description

This command is used to display VLAN trunking information.

Parameters

None.

Restrictions

None.

Example

To display the current VLAN trunking information:

```
DGS-3200-10:4#show vlan_trunk
Command: show vlan_trunk

VLAN Trunk             :Enable
VLAN Trunk Port        :1-5,7

DGS-3200-10:4#
```

35 Link Aggregation Command List

create link_aggregation group_id <value> {type [lacp | static] }
delete link_aggregation group_id <value>
config link_aggregation group_id <value 1-12> {master_port <port> | ports <portlist> | state [enable | disable] | trap [enable | disable]}
config link_aggregation algorithm [mac_source_dest | ip_source_dest]
show link_aggregation {group_id <value 1-12> | algorithm}

35-1 create link_aggregation group_id

Purpose

To create a link aggregation group on the switch.

Format

create link_aggregation group_id <value> {type [lacp | static] }

Description

This command is used to create a link aggregation group.

Parameters

Parameters	Description
group_id	Specify the group ID. The group number identifies each of the groups. The group ID is between 1 and 5 for DGS-3200-10, between 1 and 8 for DGS-3200-16, and between 1 and 12 for DGS-3200-24.
type	Specify the group type belongs to static or LACP. If the type is not specified, the default is the static type.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a link aggregation group:

```
DGS-3200-10:4#create link_aggregation group_id 1 type lacp
Command: create link_aggregation group_id 1 type lacp


Success


DGS-3200-10:4#
```

35-2 delete link_aggregation group_id

Purpose

To delete a previously configured link aggregation group.

Format

delete link_aggregation group_id <value>

Description

This command is used to delete a previously configured link aggregation group.

Parameters

Parameters	Description
group_id	Specify the group ID. The group number identifies each of the groups. The group ID is between 1 and 5 for DGS-3200-10, between 1 and 8 for DGS-3200-16, and between 1 and 12 for DGS-3200-24.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a link aggregation group:

```
DGS-3200-10:4#delete link_aggregation group_id 3
Command: delete link_aggregation group_id 3

Success.

DGS-3200-10:4#
```

35-3 config link_aggregation group_id

Purpose

To configure a previously created link aggregation group.

Format

config link_aggregation group_id <value 1-5> {master_port <port> | ports <portlist> | state [enable | disable] | trap [enable | disable]} [DGS-3200-10 Only]

config link_aggregation group_id <value 1-8> {master_port <port> | ports <portlist> | state [enable | disable] | trap [enable | disable]} [DGS-3200-16 Only]

config link_aggregation group_id <value 1-12> {master_port <port> | ports <portlist> | state [enable | disable] | trap [enable | disable]} [DGS-3200-24 Only]

Description

This command is used to configure a link aggregation group that was created with the **create link_aggregation** command above.

Parameters

Parameters	Description
group_id	Specify the group ID. The group number identifies each of the groups. The group ID is between 1 and 5 for DGS-3200-10, between 1 and 8 for DGS-3200-16, and between 1 and 12 for DGS-3200-24.
master_port	The master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port.
ports	Specify a range of ports that will belong to the link aggregation group.
state	Enable or disable the specified link aggregation group. If configuring an LACP group, the ports' state machine will start.
trap	When set to enable, Link Up and Link Down notifications are enabled for this link aggregation group. When set to disable, Link Up and Link Down notifications are disabled for link aggregation group. By default, the trap status for a link aggregation group is disabled.

Restrictions

Only Administrator-level users can issue this command.

Example

To define a load-sharing group of ports, group-id 1, master port 7:

```
DGS-3200-10:4#config link_aggregation group_id 1 master_port 7 ports 5-7
Command: config link_aggregation group_id 1 master_port 7 ports 5-7


Success.


DGS-3200-10:4#
```

35-4 config link_aggregation algorithm

Purpose

To configure the link aggregation algorithm.

Format

config link_aggregation algorithm [mac_source_dest | ip_source_dest]

Description

This command is used to configure the part of the packet examined by the switch when selecting the egress port for transmitting load-sharing data. This feature is only available when using the address-based load-sharing algorithm.

Parameters

Parameters	Description
mac_source_dest	Indicate that the switch should examine the MAC source and destination address.
ip_source_dest	Indicate that the switch should examine the IP source and destination address.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the link aggregation algorithm for mac-source-dest:

```
DGS-3200-10:4#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3200-10:4#
```

35-5 show link_aggregation

Purpose

To display the current link aggregation configuration on the Switch.

Format

show link_aggregation {group_id <value 1-5> | algorithm} **[DGS-3200-10 Only]**

show link_aggregation {group_id <value 1-8> | algorithm} **[DGS-3200-16 Only]**

show link_aggregation {group_id <value 1-12> | algorithm} **[DGS-3200-24 Only]**

Description

This command is used to display the current link aggregation configuration of the switch. If no parameter is specified, the system will display all the link aggregation information.

Parameters

Parameters	Description
group_id	Specify the group ID. The group number identifies each of the groups.

	The group ID is between 1 and 5 for DGS-3200-10, between 1 and 8 for DGS-3200-16, and between 1 and 12 for DGS-3200-24.
algorithm	Specify the display of link aggregation by the algorithm in use by that group.

Restrictions

None.

Example

To display the current link aggregation configuration when link aggregation is enabled:

```
DGS-3200-10:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 7
Member Port   : 5-8
Active Port   :
Status        : Enabled
Trap          : Disabled

Total Entries : 1

DGS-3200-10:4#
```

To display the current link aggregation configuration when link aggregation is disabled:

```
DGS-3200-10:4#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID      : 1
Type          : LACP
Master Port   : 7
Member Port   : 5-8
Active Port   :
Status        : Disabled
Trap          : Disabled

Total Entries : 1

DGS-3200-10:4#
DGS-3200-10:4#
```

36 LACP Configuration Command List

config lacp_ports <portlist> mode [active|passive]
show lacp_ports {<portlist>}

36-1 config lacp_ports

Purpose

To configure the current mode of LACP of port .

Format

config lacp_ports <portlist> mode [active|passive]

Description

This command is used to configure per-port LACP mode.

Parameters

Parameters	Description
portlist	Specified a range of ports to be configured.
mode	**active/passive**

Restrictions

Only Administrator-level users can issue this command.

Example

To configure port LACP mode for ports 1 to 10:

```
DGS-3200-10:4#config lacp_port 1-10 mode active
Command: config lacp_port 1-10 mode active


Success.


DGS-3200-10:4#
```

36-2 show lacp_ports

Purpose

To display the current mode of LACP of port(s).

Format

show lacp_ports <portlist>

Description

This command is used to display per-port LACP mode. If no parameter is specified, the system will display current LACP and all port status.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.

Restrictions

None.

Example

To display the current port LACP mode for all ports on the switch:

```
DGS-3200-10:4#show lacp_ports
Command: show lacp_ports

Port    Activity
------  --------
1       Active
2       Active
3       Active
4       Active
5       Active
6       Active
7       Active
8       Active
9       Active
10      Active

DGS-3200-10:4#
```

37 Traffic Segmentation Command List

config traffic_segmentation [<portlist>|all] forward_list[null|all|<portlist>]
show traffic_segmentation {<portlist>}

37-1 config traffic_segmentation

Purpose

To configure traffic segmentation.

Format

config traffic_segmentation [<portlist>|all] forward_list [null | all | <portlist>]

Description

This command is used to configure traffic segmentation.

Parameters

Parameters	Description	
portlist	Specify a range of ports to be configured.	
forward_list	Specify a range of ports for the forwarding list.	
	null	Specify no ports to be configured.
	all	Specify all ports to be configured.
	portlist	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command. The forwarding domain is restricted to Bridge Traffic only.

Example

To configure traffic segmentation:

```
DGS-3200-10:4# config traffic_segmentation 1-6 forward_list 7-8
Command: config traffic_segmentation 1-6 forward_list 7-8

Success.

DGS-3200-10:4#
```

37-2 show traffic_segmentation

Purpose

To display the current traffic segmentation table.

Format

show traffic_segmentation {<portlist>}

Description

This command is used to display the traffic segmentation table. If no parameter is specified, the system will display all current traffic segmentation tables.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Example

To display the traffic segmentation table:

```
DGS-3200-10:4#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------------------
1       1-10
2       1-10
3       1-10
4       1-10
5       1-10
6       1-10
7       1-10
8       1-10
9       1-10
10      1-10

DGS-3200-10:4#
```

38 Port Security Command List

config port_security ports [<portlist>| all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}
delete port_security_entry vlan_name<vlan_name 32> port <port> mac_address <macaddr>
clear port_security_entry port <portlist>
show port_security {ports <portlist>}
enable port_security trap_log
disable port_security trap_log

38-1 config port_security

Purpose

To configure port security.

Format

config port_security ports [<portlist>| all] {admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]}

Description

This command is used to configure port security. It includes admin state, maximum learning address, and lock address mode.

Parameters

Parameters	Description	
portlist	Specify a range of ports to be configured.	
all	Specify that all ports are to be configured.	
admin_state	Allow the port security to be enabled or disabled for the ports specified in the port list.	
max_learning_addr	The maximum number of address learning set to the ports specified in the portlist. The maximum number of entries is 64.	
lock_address_mode	Indicate locking address mode.	
	Permanent	Not until the secured addresses are deleted, the locked addresses will not be aged out after aging timer expires.
	DeleteOnTimeout	The locked addresses can be aged out after aging timer expire

	DeleteOnReset	Never age out the locked addresses unless restart the system to prevent from port movement or intrusion.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the port security setting for port 6:

```
DGS-3200-10:4#config port_security ports 6 admin_state enable max_learning_addr
10 lock_address_mode Permanent
Command: config port_security ports 6 admin_state enable max_learning_addr 16
lock_address_mode Permanent

Success.

DGS-3200-10:4#
```

38-2 delete port_security_entry

Purpose

To delete a port security entry by MAC address, port number, and VLAN name.

Format

delete port_security_entry vlan_name <vlan_name 32> port <port> mac_address <macaddr>

Description

This command is used to delete a port security entry by MAC address, port number, and VLAN name.

Parameters

Parameters	Description
vlan_name 32	The VLAN name the port belongs to.
mac_address	The MAC address to be deleted which was learned by the port.
port	The port number which has learned the MAC .

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a default route from the routing table for port 6:

```
DGS-3200-10:4#delete port_security_entry vlan_name default port 6 mac_address
00-01-30-10-2C-C7
Command: delete port_security_entry vlan_name default port 6 mac_address
00-01-30-10-2C-C7

Success.

DGS-3200-10:4#
```

38-3 clear port_security_entry

Purpose

To clear the MAC entries learned from the specified port(s) for the port security function.

Format

clear port_security_entry port <portlist>.

Description

This command is used to clear the MAC entries learned from the specified port(s) for the port security function.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear port security entry for port 6:

```
DGS-3200-10:4#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3200-10:4#
```

38-4 show port_security

Purpose

To display the port security related information of the switch ports.

Format

show port_security {ports <portlist>}

Description

This command is used to display the port security related information of the switch ports including the port security admin state, the maximum number of learning addresses, and the lock mode.

Parameters

None.

Restrictions

None.

Examples

To display the port security information of switch ports 1 to 6:

```
DGS-3200-10:4# show port_security ports 1-6
Command: show port_security ports 1-6

Port_security Trap/Log : Enabled

Port    Admin State  Max. Learning Addr.  Lock Address Mode
------  -----------  -------------------  -----------------
1     Disabled     1                    DeleteOnReset
2     Disabled     1                    DeleteOnReset
3     Disabled     1                    DeleteOnReset
4     Disabled     1                    DeleteOnReset
5     Disabled     1                    DeleteOnReset
6     Enabled      10                   Permanent

DGS-3200-10:4#
```

38-5 enable port_security trap_log

Purpose

To enable the port security trap/log.

Format

enable port_security trap_log

Description

This command is used to enable port security traps/logs. When this command is enabled, if there's a new

MAC that violates the pre-defined port security configuration, a trap will be sent out with the MAC and port information and the relevant information will be logged.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable a port security trap:

```
DGS-3200-10:4# enable port_security trap_log
Command: enable port_security trap_log

Success.

DGS-3200-10:4#
```

38-6 disable port_security trap_log

Purpose

To disable a port security trap/log.

Format

disable port_security trap_log

Description

This command is used to disable a port security trap/log. If the port security trap is disabled, no trap will be sent out for MAC violations.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To prevent a port security trap from being sent from the switch:

```
DGS-3200-10:4# disable port_security trap_log
Command: disable port_security trap_log

Success.

DGS-3200-10:4#
```

39 Static MAC-based VLAN Command List

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>] }
show mac_based_vlan {mac_address <macaddr> | vlan <vlan_name 32>|<vlanid <vlanid 1-4094>}

39-1 create mac_based_vlan

Purpose

To create a static MAC-based VLAN entry.

Format

create mac_based_vlan mac_address <macaddr> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Description

This command is used to create static MAC-based VLAN entries. When an entry is created for a port, the port will automatically become the untagged member port of the specified VLAN. When a static MAC-based VLAN entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentication function operating on this port.

Parameters

Parameters	Description
mac_address	The MAC address.
vlan	The VLAN to be associated with the MAC address.
vlanid	The VLAN ID to be associated with the MAC address.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a static MAC-based VLAN entry:

```
DGS-3200-10:4# create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Success.

DGS-3200-10:4#
```

39-2 delete mac_based_vlan

Purpose

To delete a static MAC-based VLAN entry.

Format

delete mac_based_vlan {mac_address <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>] }

Description

This command is used to delete a database entry. If the MAC address and VLAN are not specified, all static entries associated with the port will be removed.

Parameters

Parameters	Description
mac_address	The MAC address.
vlan	The VLAN to be associated with the MAC address.
vlanid	The VLAN ID to be associated with the MAC address.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a static MAC-based VLAN entry:

```
DGS-3200-10:4# delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Success.

DGS-3200-10:4#
```

39-3 show mac_based_vlan

Purpose

To display a static MAC-based VLAN entry.

Format

show mac_based_vlan {mac_address <macaddr> | vlan <vlan_name 32>|<vlanid <vlanid 1-4094>}

Description

This command is used to display the static MAC-based VLAN entry.

Parameters

Parameters	Description
mac_address vlan	Specify the entry to display.
vlanid	The VLAN ID to be associated with the MAC address.

Restrictions

None.

Example

In the following example, MAC address "00-80-c2-33-c3-45" is assigned to VLAN 300 by manual configuration. It is assigned to VLAN 400 by MAC-AC. Since MAC AC has higher priority than manual configuration, the manually configured entry will become inactive. To display the MAC-based VLAN entry:

```
DGS-3200-10:4# show mac_based_vlan

    MAC Address          VLAN           Status         Type
------------------  ------------  ----------- --------
00-80-e0-14-a7-57     200             Active         Static
00-80-c2-33-c3-45     300             Inactive       Static
00-80-c2-33-c3-45     400             Active         MAC AC
00-a2-44-17-32-98     400             Active         WAC

Total Entries : 4

DGS-3200-10:4#
```

40 Port Egress Filter Command List

config egress_filter ports [<portlist> | all] { unicast [enable|disable] | multicast [enable| disable] }
show egress_filter ports {<portlist>}

40-1 config egress_filter ports

Purpose

To configure the state of egress filtering on a specific port.

Format

config egress_filter ports [<portlist> | all] { unicast [enable|disable] | multicast [enable| disable] }

Description

This command is used to configure the state of egress filters on specified ports.

Parameters

Parameters	Description
portlist	Specify the portlist.
unicast	Specify the egress filter state of destination lookup fail packets. **disable**: Unknown unicast packets are not filtered and may be forwarded to this port. **enable**: Unknown unicast packets are filtered and are not forwarded to this port.
multicast	Specify the egress filter state of unregistered multicast packets. **disable**: Unregistered multicast packets are not filtered and may be forwarded to this port. **enable**: Unregistered multicast packets are filtered and are not forwarded to this port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an egress filter:

```
DGS-3200-10:4# config egress_filter 6 unicast enable multicast enable
Command: config egress_filter 6 unicast enable multicast enable

Success.

DGS-3200-10:4#
```

40-2 show egress_filter ports

Purpose

To display the port egress filter configuration.

Format

show egress_filter ports {<portlist>}

Description

This command is used to show port egress filter configuration.

Parameters

Parameters	Description
portlist	Specify the port list.

Restrictions

None.

Examples

To display the egress filter for port 6:

```
DGS-3200-10:4# show  egress_filter ports 6
Command: show egress_filter ports 6

Port    Unicast    Multicast
----    -------    -----------
6       Enabled    Enabled

DGS-3200-10:4#
```

41 BPDU Attack Protection Command List

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}
config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]
config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]
enable bpdu_protection
disable bpdu_protection
show bpdu_protection {ports {<portlist>}}

41-1 config bpdu_protection ports

Purpose

To configure port state and mode for BPDU protection.

Format

config bpdu_protection ports [<portlist> | all] {state [enable | disable] | mode [drop | block | shutdown]}

Description

This command is used to configure the BPDU protection function for the ports on the Switch. In general, there are two states, normal and under attach, in BPDU protection function. The under attack state have three modes: drop, block, and shutdown. A BPDU protection enabled port will enter under attack state when it receives one STP BPDU packet. And it will take action based on the configuration. Thus, BPDU protection can only be enabled on SPT-disabled port.

BPDU protection has higher priority than fbpdu setting configured by configure STP command in determination of BPDU handling. That is, when fbpbu is configured to forward STP BPDU but BPDU protection is enabled, then the port will not forward STP BPDU.

BPDU protection also has higher priority than BPDU tunnel port setting in determination of BPDU handling. That is, when a port is configured as BPDU tunnel port for STP, it will forward STP BPDU. But if the port is BPDU protection enabled. Then the port will not forward STP BPDU.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.
all	Specify all ports to be configured.
state	Enable or disable the BPDU protection.
mode	Specify the BPDU protection mode. The default mode is shutdown.

	drop - Specify to drop all received BPDU packets when the port enters the under attack state. **block** - Specify to drop all packets (include BPDU and normal packets) when the port enters the under attack state. **shutdown** - Specify to shut down the port when the port enters the under attack state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port state to enable and drop mode:

```
DGS-3200-10:4# config bpdu_protection ports 1 state enable mode drop
Command: config bpdu_protection ports 1 state enable mode drop

Success.

DGS-3200-10:4#
```

41-2 config bpdu_protection recovery_timer

Purpose

To configure BPDU protection recovery timer.

Format

config bpdu_protection recovery_timer [<sec 60-1000000> | infinite]

Description

This command is used to configure BPDU protection recovery timer. When a port enters the under attack state, it can be disabled or blocked based on the configuration. The state can be recovered manually or by the auto recovery mechanism. This command is used to configure the auto-recovery timer. To manually recover the port, the user needs to disable and re-enable the port.

Parameters

Parameters	Description
<sec 60-1000000>	Specify the timer (in seconds) used by the Auto-recovery mechanism to recover the port. The valid range is 60 to 1000000. Auto-recovery time is 60 seconds by default.
infinite	Specify the port that will not be auto recovered.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the BPDU protection recovery timer to 120 seconds for the Switch:

```
DGS-3200-10:4# config bpdu_protection recovery_timer 120
Command: config bpdu_protection recovery_timer 120

Success.

DGS-3200-10:4#
```

41-3 config bpdu_protection

Purpose

To configure the BPDU protection trap state or log state.

Format

config bpdu_protection [trap | log] [none | attack_detected | attack_cleared | both]

Description

This command is used to configure the BPDU protection trap state or log state.

Parameters

Parameters	Description
trap	Specify the trap state.
log	Specify the log state.
none	Specify neither **attack_detected** nor **attack_cleared** is trapped or logged.
attack_detected	Specify events will be logged or trapped when the BPDU attacks is detected.
attack_cleared	Specify events will be logged or trapped when the BPDU attacks is cleared.
both	Specify the events of attack_detected and attack_cleared shall be trapped or logged.

Restrictions

Only Administrator-level users can issue this command.

Examples

To config the bpdu_protection trap state as both for the entire switch:To configure the BPDU protection

trap state as both for the Switch:

```
DGS-3200-10:4# config bpdu_protection trap both
Command: config bpdu_protection trap both

Success.

DGS-3200-10:4#
```

41-4 enable bpdu_protection

Purpose

To enable BPDU protection globally for the Switch.

Format

enable bpdu_protection

Description

This command is used to enable BPDU protection globally for the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable BPDU protection for the Switch:

```
DGS-3200-10:4# enable bpdu_protection
Command: enable bpdu_protection

Success.

DGS-3200-10:4#
```

41-5 disable bpdu_protection

Purpose

To disable BPDU protection globally for the Switch.

Format

disable bpdu_protection

Description

This command is used to disable BPDU protection globally for the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable BPDU protection:

```
DGS-3200-10:4# disable bpdu_protection
Command: disable bpdu_protection

Success.

DGS-3200-10:4#
```

41-6 show bpdu_protection

Purpose

To display BPDU protection global configuration or per port configuration and current status.

Format

show bpdu_protection {ports {<portlist>}}

Description

This command is used to display BPDU protection global configuration or per port configuration and current status.

Parameters

Parameters	Description
ports	Specify all ports to be displayed.
<Portlist>	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display BPDU protection information:

```
DGS-3200-10:4# show bpdu_protection
Command: show bpdu_protection

BPDU Protection Global Settings
---------------------------------------
BPDU Protection Status      : Disabled
BPDU Protection Recover Time  : 60 seconds
BPDU Protection Trap State   : None
BPDU Protection Log State    : Both

DGS-3200-10:4#
```

To display BPDU protection status for ports 1 to 3:

```
DGS-3200-10:4# show bpdu_protection ports 1-3
Command: show bpdu_protection ports 1-3

Port  State        Mode       Status
----- -----------  ---------- -----------
1     Disabled    Shutdown   Normal
2     Disabled    Shutdown   Normal
3     Disabled    Shutdown   Normal

DGS-3200-10:4#
```

42 Layer 2 Protocol Tunneling (L2PT) Command List

config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp|gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]} | all] {threshold <value 0-65535>} |nni | none]
show l2protocol_tunnel {[uni | nni]}
enable l2protocol_tunnel
disable l2protocol_tunnel

42-1 config l2protocol_tunnel

Purpose

To configure Layer 2 protocol tunneling on ports.

Format

config l2protocol_tunnel ports [<portlist> | all] type [uni tunneled_protocol [{stp|gvrp | protocol_mac [01-00-0C-CC-CC-CC | 01-00-0C-CC-CC-CD]} | all] {threshold <value 0-65535>} |nni | none]

Description

This command is used to configure Layer 2 protocol tunneling on ports. Layer 2 protocol tunneling is used to tunnel Layer 2 protocol packet. If a Layer 2 protocol is tunnel-enabled on an UNI, once received the PDU on this port, the multicast destination address of the PDU will be replaced by Layer 2 protocol tunneling multicast address. The Layer 2 protocol tunneling multicast address for STP is 01-05-5D-00-00-00, for GVRP is 01-05-5D-00-00-21, for Layer 2 protocols MAC 01-00-0C-CC-CC-CC is 01-05-5D-00-00-10 and for protocol MAC 01-00-0C-CC-CC-CD is 01-05-5D-00-00-11.
When QinQ is enabled, an S-TAG will be added to the Layer 2 PDU too. The S-TAG is assigned according QinQ VLAN configuration.

Parameters

Parameters	Description
ports	Specify the ports on which the Layer 2 protocol tunneling will be configured. If specified all, all ports on the switch will be configured.
type	Specify the type of the ports. **uni** - Specify the ports as UNI ports. **nni** - Specify the ports as NNI ports. **none -** Disable tunnel on it. By default, a port is none port.

tunneled_protocol	Specify tunneled protocols on the UNI ports. **stp** - Specify to use the STP protocol. **gvrp** - Specify to use the GVRP protocol. **protocol_mac** - Specify the destination MAC address of the L2 protocol packets that will tunneled on these UNI ports. The MAC address can be 01-00-0C-CC-CC-CC or 01-00-0C-CC-CC-CD. **all** - All tunnel-abled Layer 2 protocols will be tunneled on the ports.
threshold	Specify the drop threshold for packets-per-second accepted on the UNI ports. The ports drop the PDU if the protocol's threshold is exceeded. The range of the threshold value is 0 to 65535 (packet/second). The value 0 means no limit. By default, the value is 0.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the STP tunneling on ports 1-4:

```
DGS-3200-10:4# config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp
Command: config l2protocol_tunnel ports 1-4 type uni tunneled_protocol stp

Success.

DGS-3200-10:4#
```

42-2 show l2protocol_tunnel

Purpose

To display Layer 2 protocol tunneling information.

Format

show l2protocol_tunnel {[uni | nni]}

Description

This command is used to display Layer 2 protocol tunneling information.

Parameters

Parameters	Description
uni	Specify to show UNI detail information, include tunneled and dropped PDU statistic.
nni	Specify to show NNI detail information, include de-capsulated Layer 2 PDU statistic.

Restrictions

None.

Examples

To show Layer 2 protocol tunneling information summary:

```
DGS-3200-10:4# show l2protocol_tunnel
Command: show l2protocol_tunnel

Global State: Enabled
UNI Ports: 1-2
NNI Ports: 3-4

DGS-3200-10:4#
```

To show Layer 2 protocol tunneling detail information on the UNI ports:

```
DGS-3200-10:4# show l2protocol_tunnel uni
Command: show l2protocol_tunnel uni

UNI   Tunneled            Threshold
Port  Protocol           (packet/sec)
---  -------------------  ------------
1    STP               10
     GVRP               0
     01-00-0C-CC-CC-CC  0
     01-00-0C-CC-CC-CD  0
2     STP               20
     GVRP               0
DGS-3200-10:4#
```

To show Layer 2 protocol tunneling detail information on the NNI ports:

```
DGS-3200-10:4# show l2protocol_tunnel nni
Command: show l2protocol_tunnel nni

NNI    Protocol
Port
----   -----------------
1      STP
       GVRP
```

```
       01-00-0C-CC-CC-CC
       01-00-0C-CC-CC-CD
2      STP
        GVRP
       01-00-0C-CC-CC-CC
       01-00-0C-CC-CC-CD


DGS-3200-10:4#
```

42-3 enable l2protocol_tunnel

Purpose

To enable the Layer 2 protocol tunneling function.

Format

enable l2protocol_tunnel

Description

This command is used to enable the Layer 2 protocol tunneling function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the Layer 2 protocol tunneling function:

```
DGS-3200-10:4#enable l2protocol_tunnel
Command: enable l2protocol_tunnel


Success.


DGS-3200-10:4#
```

42-4 disable l2protocol_tunnel

Purpose

To disable the L2PT function globally on the Switch.

Format

disable l2protocol_tunnel

Description

This command is used to disable the L2PT function globally on the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the Layer 2 protocol tunneling function:

```
DGS-3200-10:4# disable l2protocol_tunnel

Command: disable l2protocol_tunnel


Success.


DGS-3200-10:4#
```

43 LLDP Command List

enable lldp
disable lldp
config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]
config lldp notification_interval <sec 5-3600>
config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp }] [enable | disable] | dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable | disable]]
config lldp forward_message [enable | disable]
show lldp
show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}
show lldp ports {<portlist>}
show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}
show lldp statistics
show lldp statistics ports {<portlist>}
config lldp_med fast_start repeat_count <value 1-10>
config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]
config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | inventory}] state [enable | disable]
config lldp_med log state [enable | disable]
show lldp_med
show lldp_med ports {<portlist>}
show lldp_med local_ports
show lldp_med remote_ports {<portlist>}

43-1 enable lldp

Purpose

To enable LLDP.

Format

enable lldp

Description

This command is used to enable LLDP. This is a global control for the LLDP function. When this function is enabled, the switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP setting. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table.The default state for LLDP is disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable LLDP:

```
DGS-3200-10:4#enable lldp
Command: enable lldp

Success.

DGS-3200-10:4#
```

43-2 disable lldp

Purpose

To disable LLDP.

Format

disable lldp

Description

This command is used to disable LLDP. The Switch will stop the sending and receiving of LLDP advertisement packets.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable LLDP:

```
DGS-3200-10:4#disable lldp
Command: disable lldp

Success.

DGS-3200-10:4#
```

43-3 config lldp

Purpose

To configure LLDP timer values.

Format

config lldp [message_tx_interval <sec 5-32768> | message_tx_hold_multiplier <int 2-10> | tx_delay <sec 1-8192> | reinit_delay <sec 1-10>]

Description

This command is used to configure LLDP timer values. The message TX interval controls how often active ports retransmit advertisements to their neighbors. The message TX hold multiplier is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. The TTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). On the partner switch, when the time-to-live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB. The TX delay is used to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The TX delay defines the minimum interval between sending of LLDP messages due to the constantly changing MIB content. A re-enabled LLDP port will wait for the reinit delay after the last disable command before reinitializing.

Parameters

Parameters	Description
message_tx_interval	Specify the message TX interval between consecutive transmissions of LLDP advertisements on any given port.

message_tx_hold_multiplier	Specify the message TX hold multiplier.
tx_delay	Specify the TX delay time.
reinit_delay	Specify the reinit delay time.

Restrictions

Only Administrator-level users can issue this command.

Examples

To change the packet transmission interval:

```
DGS-3200-10:4# config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3200-10:4#
```

To change the multiplier value:

```
DGS-3200-10:4# config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_hold_multiplier 3

Success.

DGS-3200-10:4#
```

To configure the delay-interval interval::

```
DGS-3200-10:4# config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DGS-3200-10:4#
```

To change the re-initialization delay interval to five seconds:

```
DGS-3200-10:4#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DGS-3200-10:4#
```

43-4 config lldp notification_interval

Purpose

To configure LLDP timer values.

Format

config lldp notification_interval <sec 5-3600>

Description

This command is used to configure LLDP timer values. This will globally change the interval between successive LLDP change notifications generated by the switch.

Parameters

Parameters	Description
<sec 5-3600>	pecify the notification interval range is from 5 to 3600 seconds. The default setting is 5 seconds.

Restrictions

Only Administrator-level users can issue this command.

Examples

To change the notification interval to 10 seconds:

```
DGS-3200-10:4#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3200-10:4#
```

43-5 config lldp ports

Purpose

To configure LLDP options by port.

Format

config lldp ports [<portlist> | all] [notification [enable | disable] | admin_status [tx_only | rx_only | tx_and_rx | disable] | mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] [enable | disable] | basic_tlvs [{all} | {port_description | system_name | system_description | system_capabilities}] [enable | disable] | dot1_tlv_pvid [enable | disable] | dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vidlist>] [enable | disable] | dot1_tlv_protocol_identity [all | {eapol | lacp | gvrp | stp }] [enable | disable] |

dot3_tlvs [{all} | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable | disable]]

Description

This command is used to configure LLDP options by port. Enable or disable each port for sending change notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove.
The admin status options enable to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
The config management address command specifies whether system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface, associated with each management address. The interface for that management address will be also advertised in the if-index form.
An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type include four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type cannot be disabled. There are also four data types which can be optionally selected. They are port_description, system_name, system_description, and system_capability.
Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port vlan ID TLV data types from outbound LLDP advertisements.
Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.
Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.
Configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements. This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity are enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be configured.

all	Specify to configure all the ports on the system.
notification	Enable or disable the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
admin_status	Select the desired administrative per port state. The default per port state is tx_and_rx. **tx_only** - Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices. **rx_only** - Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors. **tx_and_rx** - Configure the specified port(s) to both transmit and receive LLDP packets. **disable** - Disable LLDP packet transmit and receive on the specified port(s).
mgt_addr	The port types specified for advertising indicated management address instance. **ipv4** - Specify the IP address of IPv4. **ipv6** - Specify the IP address of IPv6. **enable** - Enable port(s) specified for advertising indicated management address instance. **disable** - Disable port(s) specified for advertising indicated management address instance.
basic_tlvs	Configure an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements. **all** - Configure all four TLV data types listed below. **port_description** - This TLV optional data type indicates that LLDP agent should transmit “Port Description TLV” on the port. The default state is disabled. **system_name** - This TLV optional data type includes indicates that LLDP agent should transmit “System Name TLV.” The default state is disabled. **system_description** - This TLV optional data type includes indicates that LLDP agent should transmit “System Description TLV.” The default state is disabled. **system_capabilities** - This TLV optional data type includes indicates that LLDP agent should transmit “System Capabilities TLV.” The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled. **enable** - Enable configuration of an individual port or group of ports to

	exclude one or more of optional TLV data types from outbound LLDP advertisements. **disable** - Disable configuration of an individual port or group of ports to exclude one or more of optional TLV data types from outbound LLDP advertisements.
dot1_tlv_pvid	This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.
dot1_tlv_protocol_vid	This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled. **vlan** - Specify a VLAN to be transmitted. **vlanid** - Specify a VLAN ID list to be transmitted. **enable** - Enable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements. **disable** - Disable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.
dot1_tlv_vlan_name	This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN ID will be advertised. The default state is disabled. **vlan** - (Optional) Specify a VLAN to be transmitted. **vlanid** - (Optional) Specify a VLAN ID list to be transmitted. **enable** - Enable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements. **disable** - Disable configuration of an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.
dot1_tlv_protocol_identity	This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network, such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations which are responsible for maintaining the topology and

	connectivity of the network. If EAPOL, GVRP, STP (including MSTP), and LACP protocol identity are enabled on this port and enabled to be advertised, then the protocol identity will be advertised. The default state is disabled. **all** - Advertise all of the protocols lists below. **eapol** - Advertise EAPOL. **lacp** - Advertise LACP. **gvrp** - Advertise GVRP. **stp** - Advertise STP. **enable** - Enable configuration an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements. **disable** - Disable configuration an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.
dot3_tlvs	An individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements. **all** – (Optional) Configure all of the TLV optional data types below. **mac_phy_configuration_status** - (Optional) This TLV optional data type indicates that LLDP agent should transmit “MAC/PHY configuration/status TLV.” This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different duplex and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port supports the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled. **link_aggregation** - (Optional) This TLV optional data type indicates that LLDP agent should transmit “Link Aggregation TLV.” This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in an aggregated link, and the aggregated port ID. The default state is disabled. **maximum_frame_size** - (Optional) This TLV optional data type indicates that LLDP agent should transmit “Maximum-frame-size TLV.” The default state is disabled. **enable** - Enable the configuration of an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types

	from outbound LLDP advertisements. **disable** - Disable the configuration of an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.

Restrictions

Only Administrator-level users can issue this command.

Examples

To change the SNMP notification state of ports 1 to 5 to enable:

```
DGS-3200-10:4# config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DGS-3200-10:4#
```

To configure the mode of ports 1 to 5 to transmit and receive:

```
DGS-3200-10:4# config lldp ports 1-5 admin_status tx_and_rx
Command: config lldp ports 1-5 admin_status tx_and_rx

Success.

DGS-3200-10:4#
```

To enable ports 1 to 5 to manage address entries:

```
DGS-3200-10:4# config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable
Command: config lldp ports 1-5 mgt_addr ipv4 192.168.254.10 enable

Success.

DGS-3200-10:4#
```

To exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3200-10:4# config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3200-10:4#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3200-10:4# config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3200-10:4#
```

To exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3200-10:4# config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

DGS-3200-10:4#
```

To exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3200-10:4# config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

DGS-3200-10:4#
```

To exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3200-10:4# config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3200-10:4#
```

To exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3200-10:4# config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DGS-3200-10:4#
```

43-6 config lldp forward_message

Purpose

To configure LLDP forwarding messages.

Format

config lldp forward_message [enable | disable]

Description

This command is used to configure LLDP forwarding messages. When LLDP is disabled and LLDP forward message is enabled, the received LLDPDU packet will be forwarded. The default state is disabled.

Parameters

Parameters	Description
enable	Specify to enable LLDP forwarding messages.
disable	Specify to disable LLDP forwarding messages.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable LLDP forwarding messages:

```
DGS-3200-10:4# config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3200-10:4#
```

43-7 show lldp

Purpose

To display LLDP.

Format

show lldp

Description

This command is used to display LLDP.

Parameters

None.

Restrictions

None.

Examples

To display LLDP:

```
DGS-3200-10:4# show lldp
Command: show lldp

LLDP System Information
   Chassis ID Subtype      : MAC Address
   Chassis ID            : 00-11-22-33-44-55
   System Name           :
   System Description      : Gigabit Ethernet Switch
   System Capabilities     : Repeater, Bridge

LLDP Configurations
   LLDP Status           : Disabled
   LLDP Forward Status     : Disabled
   Message TX Interval     : 30
   Message TX Hold Multiplier: 4
   ReInit Delay          : 2
   TX Delay              : 2
   Notification Interval    : 5

DGS-3200-10:4#
```

43-8 show lldp mgt_addr

Purpose

To display the LLDP management address information.

Format

show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}

Description

This command is used to display the LLDP management address information.

Parameters

Parameters	Description
ipv4	Specify the IPv4 address of the LLDP managament address entry.
ipv6	Specify the IPv6 address of the LLDP managament address entry.

Restrictions

None.

Examples

To display management address information:

```
DGS-3200-10:4# show lldp mgt_addr
Command: show lldp mgt_addr

Address 1 :
-----------------------------------------------------
   Subtype                        : IPv4
   Address                        : 10.19.72.38
   IF Type                        : Unknown
   OID                           : 1.3.6.1.4.1.171.10.114.1.1
   Advertising Ports                 :
Total Entries : 1

DGS-3200-10:4#
```

43-9 show lldp ports

Purpose

To display LLDP per port configuration for advertisement options.

Format

show lldp ports {<portlist>}

Description

This command is used to display LLDP per port configuration for advertisement options.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display LLDP TLV option port 1:

```
DGS-3200-10:4# show lldp ports 1
Command: show lldp ports 1

Port ID             : 1
------------------------------------------------------------
Admin Status         : TX_and_RX
Notification Status    : Disabled
Advertised TLVs Option  :
   Port Description                       Disabled
   System Name                            Disabled
   System Description                     Disabled
   System Capabilities                    Disabled
   Enabled Management Address
      (None)
   Port VLAN ID                           Disabled
Enabled Port_and_Protocol_VLAN_ID
   (None)
Enabled VLAN Name
   (None)
Enabled Protocol Identity
      (None)
   MAC/PHY Configuration/Status            Disabled
   Link Aggregation                       Disabled
   Maximum Frame Size                      Disabled

DGS-3200-10:4#
```

43-10 show lldp local_ports

Purpose

To display the per-port information currently available for populating outbound LLDP advertisements.

Format

show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}

Description

This command is used to display the per-port information currently available for populating outbound LLDP advertisements.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.
brief	Display the information in brief mode.
normal	Display the information in normal mode. This is the default display mode.
detailed	Display the information in detailed mode.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display LLDP local port information for port 1:

```
DGS-3200-10:4# show lldp local_ports 1
Command: show lldp local_ports 1

Port ID : 1
------------------------------------------------------------------------------
Port ID Subtype                          : MAC Address
Port ID                                   : 00-01-02-03-05-00
Port Description                         : D-Link DGS-3620-28SC R1.00.034
                                             Port 1 on Unit 1
Port PVID                                 : 1
Management Address Count                 : 1
PPVID Entries Count                       : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status              : (See Detail)
Link Aggregation                          : (See Detail)
Maximum Frame Size                        : 1536

DGS-3200-10:4#
```

43-11 show lldp remote_ports

Purpose

To display the information learned from the neighbor parameters.

Format

show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}

Description

This command is used to display the information learned from the neighbor parameters.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.
brief	Display the information in brief mode.
normal	Display the information in normal mode. This is the default display mode.
detailed	Display the information in detailed mode.

Restrictions

None.

Examples

To display LLDP information for remote ports 1 and 2:

```
DGS-3200-10:4# show lldp remote_ports 1-2
Command: show lldp remote_ports 1-2


Remote Entities Count : 0


DGS-3200-10:4#
```

43-12 show lldp statistics

Purpose

To display an overview of neighbor detection activity on the switch.

Format

show lldp statistics

Description

This command is used to display an overview of neighbor detection activity on the switch.

Parameters

None.

Restrictions

None.

Examples

To display LLDP statistics:

```
DGS-3200-10:4# show lldp statistics
Command: show lldp statistics


Last Change Time     : 3648
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0


DGS-3200-10:4#
```

43-13 show lldp statistics ports

Purpose

To display LLDP statistic information for individual ports.

Format

show lldp statistics ports {<portlist>}

Description

This command is used to display LLDP statistic information for individual ports.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed. When port list is not specified, information for all ports will be displayed.

Restrictions

None.

Examples

To display LLDP statistic information for port 1:

```
DGS-3200-10:4# show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
-----------------------------------------
   LLDPStatsTXPortFramesTotal        : 0
   LLDPStatsRXPortFramesDiscardTotal   : 0
   LLDPStatsRXPortFramesErrors       : 0
   LLDPStatsRXPortFramesTotal        : 0
   LLDPStatsRXPortTLVsDiscardedTotal   : 0
   LLDPStatsRXPortTLVsUnrecognizedTotal : 0
   LLDPStatsRXPortAgeoutsTotal       : 0

DGS-3200-10:4#
```

43-14 config lldp_med fast_start repeat_count

Purpose

To configure the fast start repeat count.

Format

config lldp_med fast_start repeat_count <value 1-10>

Description

This command is used to configure the fast start repeat count. When an LLDP-MED Capabilities TLV is detected for an MSAP identifier not associated with an existing LLDP remote system MIB, the application layer shall start the fast start mechanism and set the 'medFastStart' timer to 'medFastStartRepeatCount' times 1. The default value is 4.

Parameters

Parameters	Description
<value 1-10>	Specify a fast start repeat count value between 1 and 10. The default value is 4.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a LLDP-MED fast start repeat count of 5:

```
DGS-3200-10:4# config lldp_med fast_start repeat_count 5
Command: config lldp_med fast_start repeat_count 5

Success.

DGS-3200-10:4#
```

43-15 config lldp_med notification topo_change

Purpose

To enable or disable each port for sending topology change notification to configured SNMP trap receiver(s) if an endpoint device is removed or moved to another port.

Format

config lldp_med notification topo_change ports [<portlist> | all] state [enable | disable]

Description

This command is used to enable or disable each port for sending topology change notification to configured SNMP trap receiver(s) if an endpoint device is removed or moved to another port.

Parameters

Parameters	Description
ports	Specify a range of ports to be configured.
state	Specify to enable or disable the SNMP trap notification of topology change detected. The default notification state is disable.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable topology change notification on all ports:

```
DGS-3200-10:4# config lldp_med notification topo_change ports all state enable
Command: config lldp_med notification topo_change ports all state enable

Success.

DGS-3200-10:4#
```

43-16 config lldp_med ports

Purpose

To enable or disable transmitting LLDP-MED TLVs.

Format

config lldp_med ports [<portlist> | all] med_transmit_capabilities [all | {capabilities | network_policy | inventory}] state [enable | disable]

Description

This command is used to enable or disable transmitting LLDP-MED TLVs. It effectively disables LLDP-MED on a per-port basis by disabling transmission of TLV capabilities. In this case, the remote table's objects in the LLDP-MED MIB corresponding to the respective port will not be populated.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be configured.
all	Specify to select all ports to be configured.
med_transmit_capabilities	Select to send the LLDP-MED TLV capabilities specified. **all** - Select to send capabilities, network policy, and inventory. **capabilities** - Specify that the LLDP agent should transmit "LLDP-MED capabilities TLV." If a user wants to transmit LLDP-MED PDU, this TLV type should be enabled. Otherwise, this port cannot transmit LLDP-MED PDU. **network_policy** - Specify that the LLDP agent should transmit "LLDP-MED

	network policy TLV." **inventory** - Specify that the LLDP agent should transmit "LLDP-MED inventory TLV."
state	Specify to enable or disable transmitting LLDP-MED.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable transmitting all capabilities on all ports:

```
DGS-3200-10:4# config lldp_med ports all med_transmit_capabilities all state enable
Command: config lldp_med ports all med_transmit_capabilities all state enable

Success.

DGS-3200-10:4#
```

43-17 config lldp_med log state

Purpose

To configure the log state of LLDP-MED events.

Format

config lldp_med log state [enable | disable]

Description

This command is used to configure the log state of LLDP-MED events.

Parameters

Parameters	Description
enable	Specify to enable thee log state of LLDP-MED events.
disable	Specify to disable the log state for LLDP-MED events. The default is disabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the log state:

```
DGS-3200-10:4# config lldp_med log state enable
Command: config lldp_med log state enable

Success.

DGS-3200-10:4#
```

43-18 show lldp_med

Purpose

To display the general LLDP-MED configuration status.

Format

show lldp_med

Description

This command is used to display the general LLDP-MED configuration status.

Parameters

None.

Restrictions

None.

Examples

To display LLDP-MED global information:

```
DGS-3200-10:4# show lldp_med
Command: show lldp_med

LLDP-MED System Information:
    Device Class                : Network Connectivity Device
    Hardware Revision          : A1
    Firmware Revision          : 1.00.016
    Software Revision          : 2.00.006
    Serial Number              :
    Manufacturer Name          : D-Link
    Model Name                 : DGS-3200-10 Gigabit Ethernet Swi
    Asset ID                   :

LLDP-MED Configuration:
    Fast Start Repeat Count    : 4

LLDP-MED Log State:Disabled

DGS-3200-10:4#
```

43-19 show lldp_med ports

Purpose

To display the LLDP-MED per port configuration for advertisement options.

Format

show lldp_med ports {<portlist>}

Description

This command is used to display the LLDP-MED per port configuration for advertisement options.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display LLDP-MED port configuration:

```
DGS-3200-10:4# show lldp_med ports 1:1
Command: show lldp_med ports 1:1

Port ID : 1:1
------------------------------------------------------------------
Topology Change Notification Status          :  Enabled
LLDP-MED Capabilities TLV                       :  Enabled
LLDP-MED Network Policy TLV                     :  Enabled
LLDP-MED Extended Power Via MDI PSE TLV     :  Enabled
LLDP-MED Inventory TLV                          :  Enabled

DGS-3200-10:4#
```

43-20 show lldp_med local_ports

Purpose

To display the per-port LLDP-MED information currently available for populating outbound LLDP-MED advertisements.

Format

show lldp_med local_ports {<portlist>}

Description

This command is used to display the per-port LLDP-MED information currently available for populating outbound LLDP-MED advertisements.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display LLDP-MED information currently available for populating outbound LLDP-MED advertisements for port 1:

```
DGS-3200-10:4# show lldp_med local_ports 1
Command: show lldp_med local_ports 1

Port ID            : 1
------------------------------------------------------------------
```

```
LLDP-MED Capabilities Support:
   Capabilities               :Support
   Network Policy             :Support
   Location Identification    :Not Support
   Extended Power Via MDI PSE :Not Support
   Extended Power Via MDI PD  :Not Support
   Inventory                  :Support

Network Policy:
 None

DGS-3200-10:4#
```

43-21 show lldp_med remote_ports

Purpose

To display LLDP-MED information learned from neighbors.

Format

show lldp_med remote_ports {<portlist>}

Description

This command is used to display the information learned from the neighbor parameters.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display remote entry information:

```
DGS-3200-10:4# show lldp_med remote_ports 1
Command: show lldp_med remote_ports 1

Port ID : 1
------------------------------------------------------------------------------
Remote Entities Count : 1
Entity 1
  Chassis ID Subtype                  : MAC Address
```

```
Chassis ID                          : 00-01-02-03-04-00
Port ID Subtype                      : Net Address
Port ID                             : 172.18.10.11

LLDP-MED capabilities:
   LLDP-MED Device Class: Endpoint Device Class III
   LLDP-MED Capabilities Support:
      Capabilities                  : Support
      Network Policy                : Support
      Location Identification        : Support
      Extended Power Via MDI         : Support
      Inventory                     : Support
   LLDP-MED Capabilities Enabled:
     Capabilities                   : Enabled
     Network Policy                 : Enabled
     Location Identification         : Enabled
     Extended Power Via MDI          : Enabled
     Inventory                      : Enabled

Network Policy:
  Application Type : Voice
    VLAN ID                        :
    Priority                       :
    DSCP                           :
    Unknown                        : True
    Tagged                         :
 Application Type : Softphone Voice
    VLAN ID                        : 200
    Priority                       : 7
    DSCP                           : 5
    Unknown                        : False
    Tagged                         : True

  Location Identification:
    Location Subtype: CoordinateBased
      Location Information          :
    Location Subtype: CivicAddress
      Location Information          :
```

```
Extended Power Via MDI
    Power Device Type: PD Device
         Power Priority               : High
         Power Source                 : From PSE
         Power Request                : 8 Watts

  Inventory Management:
    Hardware Revision                  :
    Firmware Revision                  :
    Software Revision                  :
    Serial Number                     :
    Manufacturer Name                  :
    Model Name                        :
    Asset ID                          :

DGS-3200-10:4#
```

44 Network Load Balancing (NLB) Command List

create nlb multicast_fdb [<vlan_name 32> |vlanid <vlanid>] <macaddr>
delete nlb multicast_fdb [<vlan_name 32> |vlanid <vlanid>] <macaddr>
config nlb multicast_fdb [<vlan_name 32>|vlanid <vlanid>] <macaddr> [add | delete] <portlist>
show nlb fdb

44-1 create nlb multicast_fdb

Purpose

To create the Switch's NLB multicast FDB entry.

Format

create nlb multicast_fdb [<vlan_name 32> |vlanid <vlanid>] <macaddr>

Description

This command is used to create the Switch's NLB multicast FDB entry. The network load balancing command set is used to support the Microsoft server load balancing application where multiple servers can share the same IP address and MAC address. The requests from clients will be forwarded to all servers, but will only be processed by one of them. In multicast mode, the client use the multicast MAC address as the destination MAC to reach the server. Regarding of the mode, this destination MAC is the named the shared MAC. The server uses its own MAC address (rather than the shared MAC) as the source MAC address of the reply packet.

Parameters

Parameters	Description
<vlan_name 32>	Specify the VLAN name of the NLB multicast FDB entry. This name can be up to 32 characters long.
vlanid	Specify the VLAN ID of the NLB multicast FDB entry.
<macaddr>	Specify the MAC address of the NLB multicast FDB entry to be created.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a NLB multicast FDB entry:

```
DGS-3200-10:4# create nlb multicast_fdb default 03-bf-01-01-01-01
Command: create nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DGS-3200-10:4#
```

44-2 delete nlb multicast_fdb

Purpose

To delete the Switch's NLB multicast FDB entry.

Format

delete nlb multicast_fdb [<vlan_name 32> |vlanid <vlanid>] <macaddr>

Description

This command is used to delete the Switch's NLB multicast FDB entry.

Parameters

Parameters	Description
<vlan_name 32>	Specify the VLAN name of the NLB multicast FDB entry. This name can be up to 32 characters long.
vlanid	Specify the VLAN ID of the NLB multicast FDB entry.
<macaddr>	Specify the MAC address of the NLB multicast FDB entry to be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete NLB multicast FDB entry:

```
DGS-3200-10:4# delete nlb multicast_fdb default 03-bf-01-01-01-01
Command: delete nlb multicast_fdb default 03-bf-01-01-01-01

Success.

DGS-3200-10:4#
```

44-3 config nlb multicast_fdb

Purpose

To configure the Switch's NLB multicast FDB entry.

Format

config nlb multicast_fdb [<vlan_name 32>|vlanid <vlanid>] <macaddr> [add | delete] <portlist>

Description

This command is used to configure the Switch's NLB multicast FDB entry.

Parameters

Parameters	Description
<vlan_name 32>	Specify the VLAN name of the NLB multicast FDB entry. This name can be up to 32 characters long.
vlanid	Specify the VLAN ID of the NLB multicast FDB entry.
<macaddr>	Specify the MAC address of the NLB multicast FDB entry to be configured.
add	Specify a list of forwarding ports to be added.
delete	Specify a list of forwarding ports to be deleted.
<portlist>	Specify a list of forwarding ports to be added or deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure NLB multicast MAC forwarding database:

```
DGS-3200-10:4#config nlb multicast_fdb default 03-bf-01-01-01-01 add 1-5
Command: config nlb multicast_fdb default 03-BF-01-01-01-01 add 1-5


Success.


DGS-3200-10:4#
```

44-4 show nlb fdb

Purpose

To show the NLB configured entry.

Format

show nlb fdb

Description

This command is used to show the NLB configured entry.

Parameters

None.

Restrictions

None.

Examples

To display the NLB forwarding table:

```
DGS-3200-10:4#show nlb fdb
Command: show nlb fdb

 MAC Address      VLAN ID   Egress Ports
 ----------------- ---------- -------------------------------------------
 03-BF-01-01-01-01 1        1-5

Total Entries :1

DGS-3200-10:4#
```

VI. IP

The IP section includes the following chapters: Basic IP, Auto Config, Routing Table, ARP and Loopback Detection.

45 Basic IP Command List

config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] | dhcp_option12 [hostname <hostname 63> | clear_hostname | state [enable | disable]]]
create ipif <ipif_name 12> <vlan_name 32> {state [enable|disable]}
delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]
enable ipif [<ipif_name 12> | all]
disable ipif [<ipif_name 12> | all]
show ipif {<ipif_name 12>}
enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]
show ipif_ipv6_link_local_auto {<ipif_name 12>}

45-1 config ipif

Purpose

To configure the specified IP interface.

Format

config ipif <ipif_name 12>[{ipaddress<network_address> |vlan<vlan_name 32>| state [enable|disable]}| bootp |dhcp | ipv6 ipv6address <ipv6networkaddr>]
config ipif <ipif_name 12> [{ipaddress <network_address> | vlan <vlan_name 32> | state [enable | disable]} | bootp | dhcp | ipv6 ipv6address <ipv6networkaddr> | dhcpv6_client [enable | disable] | dhcp_option12 [hostname <hostname 63> | clear_hostname | state [enable | disable]]]

Description

This command is used to configure the specified IP interface.

Parameters

Parameters	Description
<ipif_name>	The name of the IP interface.
ipaddress	The IP address and netmask of the IP interface to be created. You can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16).

vlan	The name of the VLAN corresponding to the IP interface.
state	Allow to enable or disable the IP interface.
bootp	Allow the selection of the BOOTP protocol for the assignment of an IP address to the switch's System IP interface.
dhcp	Allow the selection of the DHCP protocol for the assignment of an IP address to the switch's System.
ipv6networkaddr	The IPv6 address and subnet prefix of the IPV6 address to be create.
dhcpv6_client	Specify to enable or disable DHCPv6 Client.
dhcp_option12	**hostname** - Specify the host name to be inserted in the DHCPDISCOVER and DHCPREQUEST message. The specified host name must start with a letter, end with a letter or digit, and have only letters, digits, and hyphen as interior characters; the maximum length is 63. **clear_hostname** – Specify to clear the hostname setting. If a host name is empty, the system name will be used to encode option 12. The length of the system is more than 63 characters. The superfluous chars will be truncated. If the system name is also empty, then the product model name will be used to encode option 12.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the System IP interface:

```
DGS-3200-10:4# config ipif System vlan v1
Command: config ipif System vlan v1

Success.

DGS-3200-10:4#
```

45-2 create ipif

Purpose

To create an IPv6 interface for IPv6 addresses.

Format

create ipif <ipif_name 12> <vlan_name 32> {state [enable|disable]}

Description

This command is used to create an IP interface for IPv6 only. This interface can only be configured with an

IPv6 address. Because only one IPV6 interface is supported, when the System interface already has some IPV6 addresses, executing this command will fail.

Note: The Switch only supports one IP interface for IPV6 addresses.

Parameters

Parameters	Description
ipif_name	The name of the interface.
vlan_name	The name of the VLAN corresponding to the IP interface.
state	The state of the IP interface.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IP interface “petrovic1”:

```
DGS-3200-10:4# create ipif ip petrovic1
Command: create ipif ipif ip petrovic1

Success.

DGS-3200-10:4#
```

45-3 delete ipif

Purpose

To delete an interface or an IPv6 address.

Format

delete ipif [<ipif_name > {ipv6address <ipv6networkaddr>} | all]

Description

This command is used to delete an IPv6 interface or an IPv6 address.

Parameters

Parameters	Description
ipif_name	The name of the interface.
ipv6networkaddr	The IPv6 network address which want to be deleted by administrator.
all	All IP interface except the System IP interface will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete interface “petrovic1.”

```
DGS-3200-10:4#delete ipif petrovic1
Command: delete ipif petrovic1

Success.

DGS-3200-10:4#
```

45-4 enable ipif

Purpose

To enable the administrative state for an interface.

Format

enable ipif [<ipif_name 12> | all]

Description

This command is used to enable the state for an IPIF. When the state is enabled, the IPv4 processing will be started when an IPv4 address is configured on the IPIF. The IPv6 processing will be started when an IPv6 address is explicitly configured on the IPIF.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All of the IP interfaces.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the state for interface “petrovic1”:

```
DGS-3200-10:4#enable ipif petrovic1
Command: enable ipif petrovic1

Success.

DGS-3200-10:4#
```

45-5 disable ipif

Purpose

To disable the administrative state for an interface.

Format

disable ipif [<ipif_name 12> | all]

Description

This command is used to disable the state of an interface.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All the IP interface

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the state for an interface:

```
DGS-3200-10:4#disable ipif petrovic1
Command: disable ipif petrovic1

Success.

DGS-3200-10:4#
```

45-6 show ipif

Purpose

To display IP interface settings.

Format

show ipif {<ipif_name 12>}

Description

This command is used to display IP interface settings. If no parameter is specified, all interface settings will be displayed.

Parameters

Parameters	Description
ipif_name	The name of the interface.

Restrictions

None.

Examples

To display IP interface settings:

```
DGS-3200-10:4#show ipif
Command: show ipif

IP Interface Settings

IP Interface                : System
IP Address                  : 10.90.90.90 (Manual)
Subnet Mask                 : 255.0.0.0
VLAN Name                   : v1
Interface Admin State       : Enabled
DHCPv6 Client State         : Disabled
Link Status                 : LinkUp
Member Ports                : 1-10
DHCP Option12 State         : Disabled
DHCP Option12 Host Name     :

Total Entries   : 1



DGS-3200-10:4#
```

45-7 enable ipif_ipv6_link_local_auto

Purpose

To enable the auto configuration of link local address when no IPv6 address is configured.

Format

enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Description

This command is used to enable the auto configuration of link local address when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be

automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All the IP interfaces.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the automatic configuration of link local address for an interface:

```
DGS-3200-10:4#enable ipif_ipv6_link_local_auto interface1
Command: enable ipif_ipv6_link_local_auto interface1

Success.

DGS-3200-10:4#
```

45-8 disable ipif_ipv6_link_local_auto

Purpose

To disable the auto configuration of link local address when no IPv6 address is configured.

Format

disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]

Description

This command is used to disable the auto configuration of link local address when no IPv6 address is explicitly configured.

Parameters

Parameters	Description
ipif_name	The name of the interface.
all	All the IP interface

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the automatic configuration of link local address for an interface.

```
DGS-3200-10:4#disable ipif_ipv6_link_local_auto interface1
Command: disable ipif_ipv6_link_local_auto interface1

Success.

DGS-3200-10:4#
```

45-9 show ipif_ipv6_link_local_auto

Purpose

To display the link local address automatic configuration state.

Format

show ipif_ipv6_link_local_auto {<ipif_name 12>}

Description

Use this command to display the link local address automatic configuration state.

Parameters

Parameters	Description
ipif_name	The name of the interface.

Restrictions

None

Examples

To display the link local address automatic configuration state:

```
DGS-3200-10:4#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System           Automatic Link Local Address: Disabled
 IPIF: interface1      Automatic Link Local Address: Enabled

DGS-3200-10:4#
```

46 Auto Config Command List

show autoconfig
enable autoconfig
disable autoconfig

46-1 show autoconfig

Purpose

To display the DHCP auto configuration status.

Format

show autoconfig

Description

This command is used to display the DHCP auto configuration status.

Restrictions

None.

Example

To display the DHCP auto configuration status:

```
DGS-3200-10:4#show autoconfig
Command: show autoconfig


Autoconfig State: Disabled


DGS-3200-10:4#
```

46-2 enable autoconfig

Purpose

To enable DHCP auto configuration.

Format

enable autoconfig

Description

This command is used to enable DHCP auto configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable DHCP auto configuration status:

```
DGS-3200-10:4#enable autoconfig
Command: enable autoconfig


Success.


DGS-3200-10:4#
```

46-3 disable autoconfig

Purpose

To disable DHCP auto configuration.

Format

disable autoconfig

Description

This command is used to disable DHCP auto configuration.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable the DHCP auto configuration status:

```
DGS-3200-10:4#disable autoconfig
Command: disable autoconfig


Success.


DGS-3200-10:4#
```

47 Routing Table Command List

create iproute default <ipaddr> {<metric 1-65535>}
delete iproute default
show iproute {<static>}
create ipv6route [default] [<ipif_name 12> <ipv6addr> |<ipv6addr>] {<metric 1-65535>}
delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr>] | all]
show ipv6route

47-1 create iproute

Purpose

To create a default IP route entry.

Format

create iproute default <ipaddr> {<metric 1-65535>}

Description

This command is used to create a default IP route entry.

Parameters

Parameters	Description
ipaddr	The IP address for the next hop router.
metric	The default setting is 1.That is, the default hop cost is 1.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a static address 10.48.74.121:

```
DGS-3200-10:4#create iproute default 10.48.74.121
Command: create iproute default 10.48.74.121

Success.

DGS-3200-10:4#
```

47-2 delete iproute default

Purpose

To delete a default IP route entry.

Format

delete iproute default

Description

This command is used to delete a default route entry.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a default route from the routing table:

```
DGS-3200-10:4#delete iproute default
Command: delete iproute default

Success.

DGS-3200-10:4#
```

47-3 show iproute

Purpose

To display the switch's current IP routing table.

Format

show iproute {<static>}

Description

This command is used to display the switch's current IP routing table.

Parameters

Parameters	Description
<static>	The static address.

Restrictions

None.

Examples

To display the contents of the IP routing table:

```
DGS-3200-10:4#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway           Interface      Hops       Protocol
------------------  ---------------   ------------   --------   --------
10.0.0.0/8          0.0.0.0           System         1          Local

Total Entries : 1

DGS-3200-10:4#
```

47-4 create ipv6route

Purpose

To create an IPv6 default route.

Format

create ipv6route [default] [<ipif_name 12> <ipv6addr>| <ipv6addr>]{<metric 1-65535>}

Description

This command is used to create an IPv6 static route. If the next hop is a global address, it is not necessary to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Parameters

Parameters	Description
default	Specify the default route.
ipif_name	Specify the interface for the route.
ipv6addr	Specify the next hop address for this route.
metric	The default setting is 1.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IPv6 default route:

```
DGS-3200-10:4#create ipv6route default System FEC0::5
Command: create ipv6route default System FEC0::5

Success.

DGS-3200-10:4#
```

47-5 delete ipv6route

Purpose

To delete an IPv6 static route.

Format

delete ipv6route [default] [<ipif_name> <ipv6addr> | <ipv6addr>] | all]

Description

This command is used to delete an IPv6 static route. If the next hop is a global address, it is not necessary to indicate the interface name. If the next hop is a link local address, then the interface name must be specified.

Parameters

Parameters	Description
default	Specify the default route.
ipv6addr	Specify the next hop address for the default route
all	All static created routes will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IPv6 static route:

```
DGS-3200-10:4#delete ipv6route default System FEC0::5
Command: delete ipv6route default System FEC0::5

Success.

DGS-3200-10:4#
```

47-6 show ipv6route

Purpose

To display IPv6 routes.

Format

show ipv6route

Description

This command is used to display IPv6 routes.

Parameters

None.

Restrictions

None.

Examples

To display an IPv6 route:

```
DGS-3200-10:4#show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                              Protocol: Static  Metric: 1
Next Hop   : FEC0::5                           IPIF    : System


Total Entries: 1


DGS-3200-10:4#
```

48 ARP Command List

create arpentry <ipaddr> <macaddr>
delete arpentry [<ipaddr> | all]
config arpentry <ipaddr> <macaddr>
config arp_aging time <value 0-65535>
clear arptable
show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static }

48-1 create arpentry

Purpose

To make a static entry in the ARP table.

Format

create arpentry <ipaddr> <macaddr>

Description

This command is used to enter an IP address and the corresponding MAC address into the switch's ARP table.

Parameters

Parameters	Description
ipaddr	The IP address of the end node or station.
macaddr	The MAC address corresponding to the IP address above.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DGS-3200-10:4#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3200-10:4#
```

48-2 delete arpentry

Purpose

To delete a static entry into the ARP table.

Format

delete arpentry [<ipaddr> | all]

Description

This command is used to delete a static ARP entry, made using the **create arpentry** command above, by specifying either the IP address of the entry or all. Specifying **all** clears the switch's ARP table.

Parameters

Parameters	Description
ipaddr	The IP address of the end node or station.
all	Delete all ARP entries

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DGS-3200-10:4#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3200-10:4#
```

48-3 config arpentry

Purpose

To configure a static entry to the ARP table.

Format

config arpentry <ipaddr> <macaddr>

Description

This command is used to configure a static entry to the ARP table. Specify the IP address and MAC address of the entry.

Parameters

Parameters	Description
ipaddr	The IP address of the end node or station.
macaddr	The MAC address corresponding to the IP address above.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a static ARP entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DGS-3200-10:4#config arpentry 10.48.74.121 00-50-BA-00-07-36
Command: config arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3200-10:4#
```

48-4 config arp_aging time

Purpose

To configure the age-out timer for ARP table entries on the switch.

Format

config arp_aging time <value 0-65535>

Description

This command is used to set the maximum amount of time, in minutes, that an ARP entry can remain in the switch's ARP table, without being accessed, before it is dropped from the table..

Parameters

Parameters	Description
value	The ARP age-out time, in minutes. The default is 20. The range is 0 to 65535.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the ARP aging time:

```
DGS-3200-10:4#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3200-10:4#
```

48-5 show arpentry

Purpose

To display the ARP table.

Format

show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static}

Description

This command is used to display the Address Resolution Protocol (ARP) table. You can filter the display by IP address, Interface name, or static entries. If no parameter is specified, all ARP entries will be displayed.

Parameters

Parameters	Description
ipif_name	The name of the IP interface the end node or station for which the ARP table entry was made, resides on.
ipaddr	The IP address of the end node or station.
static	Display the static entries from the ARP table.

Restrictions

None.

Examples

To display the ARP table:

```
DGS-3200-10:4# show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface       IP Address        MAC Address         Type
--------------  ---------------   -----------------   ---------------
System           10.0.0.0           FF-FF-FF-FF-FF-FF  Local/Broadcast
System           10.90.90.90       00-01-02-03-04-00  Local
System           10.255.255.255    FF-FF-FF-FF-FF-FF  Local/Broadcast

Total Entries: 3

DGS-3200-10:4#
```

48-6 clear arptable

Purpose

To remove dynamic entries from the ARP table.

Format

clear arptable

Description

This command is used to remove dynamic entries from the ARP table. Static ARP entries are not affected.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To remove the dynamic entries from the ARP table:

```
DGS-3200-10:4#clear arptable
Command: clear arptable

Success.

DGS-3200-10:4#
```

49 Loopback Detection Command List

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}
config loopdetect ports [<portlist>| all] state [enable | disable]
enable loopdetect
disable loopdetect
show loopdetect
show loopdetect ports {<portlist>}
config loopdetect trap [none | loop_detected | loop_cleared | both]
config loopdetect log state [enable | disable]

49-1 config loopdetect

Purpose

To configure the loop-back detection function on the switch.

Format

config loopdetect {recover_timer [<value 0> | <sec 60-1000000>] | interval <sec 1-32767> | mode [port-based | vlan-based]}

Description

This command is used to set up the loop-back detection function (LBD) for the entire switch.

Parameters

Parameters	Description
recover_timer	The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is 60 to 1000000. Zero is a special value which means to disable the auto-recovery mechanism, hence, user needs to recover the disabled port back manually. Default value of recover_timer is 60.
interval	The time interval (in seconds) at which device transmits all the CTP(Configuration Test Protocol) packets to detect the loop-back event. The default setting is 10. Valid range is 1 to 32767.
mode	Choose the loop-detection operation mode. In the port-based mode , the port will be shut-down (disabled) when detecting loop ; in vlan-based mode , the port can't process packets of the VLAN that detecting the loop.

Restriction

Only Administrator-level users can issue this command.

Examples

To set a recover time of 0 and an interval of 20 in VLAN-based mode:

```
DGS-3200-10:4# config loopdetect recover_timer 0 interval 20 mode vlan-based
Command: config loopdetect  recover_timer 0 interval 20 mode vlan-based

Success.

DGS-3200-10:4#
```

49-2 config loopdetect ports

Purpose

To configure loop-back detection function for the port on the switch.

Format

config loopdetect ports [<portlist>| all] state [enable | disable]

Description

This command is used to set up the loop-back detection function for the interface on the switch.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.
all	For setting all ports in the system, use the **all** parameter.
state	Allow loop-detect to be enabled or disabled for the ports specified in the port list. The default is disabled.

Restriction

Only Administrator-level users can issue this command.

Examples

To set up loop-back detection:

```
DGS-3200-10:4# config loopdetect ports 1-5 state enable
Command: config loopdetect ports 1-5 state enable

Success.

DGS-3200-10:4#
```

49-3 enable loopdetect

Purpose

To globally enable the loop detection function on the switch.

Format

enable loopdetect

Description

This command is used to allow the loop detection function to be globally enabled on the switch. The default value is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable loop detection:

```
DGS-3200-10:4#enable loopdetect
Command: enable loopdetect

Success.

DGS-3200-10:4#
```

49-4 disable loopdetect

Purpose

To globally disable the loop detection function on the switch.

Format

disable loopdetect

Description

This command allows the loop detection function to be globally disabled on the switch. The default value is enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable loop detection:

```
DGS-3200-10:4#disable loopdetect
Command: disable loopdetect

Success.

DGS-3200-10:4#
```

49-5 show loopdetect

Purpose

To display the switch's current loop detection configuration.

Format

show loopdetect

Description

This command is used to display the switch's current loop detection configuration.

Parameters

None.

Restrictions

None.

Examples

To display the switch's current loop detection configuration:

```
DGS-3200-10:4#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 Status          : enabled
 Mode            : VLAN-based
 Interval        : 20 sec
 Recover Time    : 60 sec
 Trap State      : None
 Log State       : Enabled



DGS-3200-10:4#
```

49-6 show loopdetect ports

Purpose

To display the switch's current per-port loop detection configuration.

Format

show loopdetect ports {<portlist>}

Description

This command is used to display the switch's current per-port loop detection configuration and status.

Parameters

Parameters	Description
ports	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display the loop detection state of ports 1 to 9 in port-based mode:

```
DGS-3200-10:4#show loopdetect  ports 1-9
Command: show loopdetect  ports 1-9

Port   Loopdetect State    Loop Status
------ ------------------ ----------
1        Enabled              Normal
2        Enabled              Normal
3        Enabled              Normal
4        Enabled              Normal
5        Enabled              Loop!
6        Enabled              Normal
7        Enabled              Loop!
8        Enabled              Normal
9        Enabled              Normal

DGS-3200-10:4#
```

To display loop detection state of ports 1 to 9 under VLAN-based mode:

```
DGS-3200-10:4#show loopdetect  ports 1-9
Command: show loopdetect  ports 1-9

Port   Loopdetect State    Loop VLAN
------ ------------------ ----------
1       Enabled            None
2       Enabled            None
3       Enabled            None
4       Enabled            None
5       Enabled            2
6       Enabled            None
7       Enabled            2
8       Enabled            None
9       Enabled            None

DGS-3200-10:4#
```

49-7 config loopdetect trap

Purpose

To configure the trap mode.

Format

config loopdetect trap [none | loop_detected | loop_cleared | both]

Description

This command is used to configure the trap mode. A loop detected trap is sent when the loop condition is detected and a loop cleared trap is sent when the loop condition is cleared.

Parameters

Parameters	Description
none	Traps will not be sent for both cases.
loop_detected	Traps are sent when the loop condition is detected
loop_cleared	Traps are sent when the loop condition is cleared.
both	Traps will be sent for both cases.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a trap:

```
DGS-3200-10:4#config loopdetect trap both
Command: config loopdetect trap both

Success.

DGS-3200-10:4#
```

49-8 config loopdetect log state

Purpose

To configure the log state for LBD. The default value is enabled.

Format

config loopdetect log state [enable | disable]

Description

This command is used to configure the log state for LBD. The default value is enabled.

Parameters

Parameters	Description
enable	Specif to enable the LBD log feature.
disable	Specif to disable the LBD log feature.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the log state for LBD:

```
DGS-3200-10:4# config loopdetect log state enable

Command: config loopdetect log state enable


Success.


DGS-3200-10:4#
```

VII. Multicast

The Multicast section includes the following chapters: IGMP Snooping, IGMP Authentication, MLD Snooping, Limited Multicast IP Address, and IGMP Snooping Multicast VLAN (ISM).

50 IGMP Snooping Command List

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]}
config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}
config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add |delete] <portlist>
config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable igmp_snooping
disable igmp_snooping
show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}
config igmp_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show igmp_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>]
create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
show igmp_snooping static_group {[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipaddr >}
show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
config igmp_snooping data_driven_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}
config igmp_snooping data_ driven _learning max_learned_entry <value 1-256>
clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipaddr> | all]]
show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
show igmp_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipaddr>]}

clear igmp_snooping statistics counter

50-1 config igmp_snooping

Purpose

To configure IGMP snooping on the switch.

Format

config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {state [enable | disable] | fast_leave [enable | disable] | report_suppression [enable | disable]}

Description

This command is used to configure IGMP snooping on the switch.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which IGMP snooping is to be configured. **all** indicates all VLANs.
vlanid	Specify the list of VLAN IDs to be configured.
state	Enable or disable IGMP snooping for the chosen VLAN.
fast_leave	Enable or disable the IGMP snooping fast leave function. If enabled, the membership is immediately removed when the system receive the IGMP leave message.
report_suppression	The Switch uses IGMP report suppression to forward only one IGMP report per multicast router query to multicast devices.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure IGMP snooping:

```
DGS-3200-10:4#config igmp_snooping vlan_name default state enable
Command: config igmp_snooping vlan_name default state enable

Success.

DGS-3200-10:4#
```

50-2 config igmp_snooping querier

Purpose

To configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members, the permitted packet loss that guarantees IGMP snooping.

Format

config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_member_query_interval <sec 1-25> | state [enable | disable] | version <value 1-3>}

Description

This command is used to configure the IGMP snooping querier.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which IGMP snooping querier is to be configured.
vlanid	Specify the list of VLAN IDs to be configured as a querier.
all	Specify to configure all VLANs as queriers.
query_interval	Specify the amount of time in seconds between general query transmissions. the default setting is 125 seconds..
max_reponse_time	The maximum time in seconds to wait for reports from members. The default setting is 10 seconds.
robustness_variable	Provide fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group member interval—Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval—Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count—Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to have a high loss.

last_member_query_interval	The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. Lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. On receiving a leave message, the router will assume there are no local members on the interface if there are no reports received after the response time (which is the last member query interval * robustness variable).
state	If the state is enable, it allows the switch to be selected as an IGMP Querier (sends IGMP query packets). It the state is disabled, then the switch can not play the role as a querier. Note that if the Layer 3 router connected to the switch provides only the IGMP proxy function but does not provide the multicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port.
version	Specifies the version of IGMP packet that will be sent by this port. If an IGMP packet received by the interface has a version higher than the specified version, this packet will be dropped.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the IGMP snooping querier:

```
 DGS-3200-10:4# config igmp_snooping querier vlan_name default query_interval 125
state enable
 Command: config igmp_snooping querier vlan_name default query_interval 125 state
enable

 Success.

 DGS-3200-10:4#
```

50-3 config router_ports

Purpose

To configure ports as router ports.

Format

config router_ports [<vlan_name 32> | vlanid <vlanid_list>] [add |delete] <portlist>

Description

This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.

Parameters

Parameters	Description
<vlan_name 32>	The name of the VLAN on which the router port resides.
vlanid	Specify a list of VLAN IDs to be configured.
add	Specify to add the router ports
delete	Specify to add or delete the router ports.
<portlist>	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set up static router ports:

```
DGS-3200-10:4#config router_ports default add 1-10
Command: config router_ports default add 1-10


Success.


DGS-3200-10:4#
```

50-4 config router_ports_forbidden

Purpose

To configure ports as forbidden router ports.

Format

config router_ports_forbidden [<vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Description

This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Parameters

Parameters	Description
<vlan_name 32>	The name of the VLAN on which the router port resides.
vlanid	Specify a list of VLAN IDs to be configured.
add	Specify to add the forbidden router ports.
delete	Specify to delete the forbidden router ports.
<portlist>	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set up port range 1 to 7 to be forbidden router ports of the default VLAN:

```
DGS-3200-10:4#config router_ports_forbidden default add 1-7
Command: config router_ports_forbidden default add 1-7

Success.

DGS-3200-10:4#
```

50-5 enable igmp_snooping

Purpose

To enable IGMP snooping on the switch.

Format

enable igmp_snooping

Description

This command allows you to enable IGMP snooping on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable IGMP snooping on the switch:

```
DGS-3200-10:4#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3200-10:4#
```

50-6 disable igmp_snooping

Purpose

To disable IGMP snooping on the switch.

Format

disable igmp_snooping

Description

This command is used to disable IGMP snooping on the switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable IGMP snooping:

```
DGS-3200-10:4#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3200-10:4#
```

50-7 show igmp_snooping

Purpose

To display the current status of IGMP snooping on the switch.

Format

show igmp_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Description

This command is used to display the current IGMP snooping configuration on the switch. If no parameter is specified, the system will display all current IGMP snooping configuration.

Parameters

Parameters	Description
vlan	Specify a name of the VLAN for which you want to view the IGMP snooping configuration.
vlanid	Specify a list of VLAN IDs for which you want to view the IGMP snooping configuration.

Restrictions

None.

Examples

To show IGMP snooping:

```
DGS-3200-10:4#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Enabled
 Data Driven Learning Max Entries        : 56

 VLAN Name                       : default
 Query Interval                  : 125
 Max Response Time               : 10
 Robustness Value                : 2
 Last Member Query Interval      : 1
 Querier State                   : Enabled
 Querier Role                    : Querier
 Querier IP                      : 10.90.90.90
 Querier Expiry Time             : 0 secs
 State                           : Enabled
 Fast Leave                      : Disabled
 Rate Limit                      : No Limitation
 Report Suppression              : Disabled
 Version                         : 3
 Data Driven Learning State      : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1


DGS-3200-10:4#
```

50-8 show igmp_snooping group

Purpose

To display the current IGMP snooping group configuration on the switch.

Format

show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipaddr>}} {data_driven}

Description

This command is used to display the current IGMP snooping group configuration on the switch. If no parameter is specified, the system will display all current IGMP
snooping group configurations of the switch.

Parameters

Parameters	Description
vlan	The name of the VLAN for which to view IGMP snooping group configuration information.
vlanid	Specify the VLAN IDs for which to view IGMP snooping group configuration information.
ports	Specify the list of ports for which to view IGMP snooping group information.
data_driven	Specify to display data-driven IGMP snooping group entries.

Restrictions

None.

Examples

To display IGMP snooping group(s):

```
DGS-3200-10:4#show igmp_snooping group
Command: show igmp_snooping group



 Source/Group                   : NULL/239.255.255.250
 VLAN Name/VID                  : default/1
 Member Ports                   : 1
 UP Time                        : 74
 Expiry Time                    : 216
 Filter Mode                    : EXCLUDE

 Total Entries: 1



DGS-3200-10:4#
```

50-9 config igmp_snooping rate_limit

Purpose

To configure the upper limit per second for ingress IGMP control packets. Packets come from both the router and member port need to do the rate limit check.

Format

config igmp_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Description

This command is used to configure the upper limit per second for ingress IGMP control packets.

Parameters

Parameters	Description
ports	Specify a range of ports to be configured.
vlanid	Specify a range of VLANs to be configured.
<value 1-1000>	Specify the rate of IGMP control packets that the Switch can process on a specific port/VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.
no_limit	Specify to have unlimited rate.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the IGMP snooping rate limit for ports 1-2 to have no limit:

```
DGS-3200-10:4#config igmp_snooping rate_limit ports 1-2 no_limit
Command: config igmp_snooping rate_limit ports 1-2 no_limit

Success.

DGS-3200-10:4#
```

50-10 show igmp_snooping rate_limit

Purpose

To display the IGMP snooping rate limit setting.

Format

show igmp_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>]

Description

This command is used to display the IGMP snooping rate limit setting.

Parameters

Parameters	Description
ports	Specify a range of ports to be displayed.
vlanid	Specify a range of VLANs to be displayed.

Restrictions

None.

Examples

To display the IGMP snooping rate limit for ports 1-2:

```
DGS-3200-10:4#show igmp_snooping rate_limit ports 1-2
Command: show igmp_snooping rate_limit ports 1-2

Port     Rate Limit
--------  ------------
1          No Limit
2          No Limit

Total Entries: 2

DGS-3200-10:4#
```

50-11 create igmp_snooping static_group

Purpose

To create an IGMP snooping multicast static group.

Format

create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Description

This command is used to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 IGMP operation. The Reserved IP multicast address 224.0.0.X must be excluded from the configured

group.The VLAN must be created first before a static group can be created.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the router port resides.
vlanid	Specify the VLAN ID list.
<ipaddr>	Specify the multicast group IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IGMP snooping static group on default VLAN, group 239.1.1.1:

```
DGS-3200-10:4#create igmp_snooping static_group vlan default 239.1.1.1
Command: create igmp_snooping static_group vlan default 239.1.1.1

Success.

DGS-3200-10:4#
```

50-12 config igmp_snooping static_group

Purpose

To configure an IGMP snooping multicast group static member port.

Format

config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>

Description

This command is used to configure an IGMP snooping static group on the switch. When a port is configured as a static member port, the IGMP protocol will not operate on this port. Therefore, suppose that a port is a dynamic member port learned by IGMP. If this port is configured as a static member later, then the IGMP protocol will stop operating on this port. The IGMP protocol will resume once this port is removed from static member ports. The static member port will only affect V2 IGMP operation.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipaddr>	Specify the multicast group IP address.

add	Specify to add the member ports.
delete	Specify to delete the member ports.
<portlist>	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add port 9 to 10 to be IGMP snooping static member ports for group 239.1.1.1 on default VLAN:

```
DGS-3200-10:4# config igmp_snooping static_group vlan default 239.1.1.1 add 9-10
Command: config igmp_snooping static_group vlan default 239.1.1.1 add 9-10

Success.

DGS-3200-10:4#
```

50-13 delete igmp_snooping static_group

Purpose

To delete an IGMP snooping multicast static group.

Format

delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>

Description

This command is used to delete an IGMP snooping static group on the switch. The deletion of an IGMP snooping static group will not affect the IGMP snooping dynamic member ports for a group.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipaddr>	Specify the multicast group IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IGMP snooping static group from the default VLAN, group 239.1.1.1:

```
DGS-3200-10:4# delete igmp_snooping static_group vlan default 239.1.1.1
Command: delete igmp_snooping static_group vlan default 239.1.1.1

Success.

DGS-3200-10:4#
```

50-14 show igmp_snooping static_group

Purpose

To display the IGMP snooping static multicast group.

Format

show igmp_snooping static_group {[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipaddr >}

Description

This command is used to display the IGMP snooping static multicast group.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipaddr>	Specify the multicast group IP address.

Restrictions

None.

Examples

To display all the IGMP snooping static groups:

```
DGS-3200-10:4#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                     IP Address      Static Member Ports
------------------------------  -------------  ----------------------
1   /default                    239.1.1.1       9-10

 Total Entries : 1



DGS-3200-10:4#
```

50-15 show igmp_snooping statistic counter

Purpose

To display the IGMP snooping statistics counter for IGMP protocol packets that are transmitted or received by the switch since IGMP snooping was enabled.

Format

show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]

Description

This command is used to display the IGMP snooping statistics counter for IGMP protocol packets that are transmitted or received by the switch since IGMP snooping was enabled.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
ports	Specify a range of ports to be configured.

Restrictions

None.

Examples

To display the IGMP snooping statistics counter for port 1:

```
DGS-3200-10:4# show igmp_snooping statistic counter ports 1
Command: show igmp_snooping statistic counter ports 1

Port #        : 1
-------------------------------------------------
Group Number    : 0

Receive Statistics
   Query
     IGMP v1 Query              : 0
     IGMP v2 Query              : 0
     IGMP v3 Query              : 0
     Total                    : 0
     Dropped By Rate Limitation     : 0
    Dropped By Multicast VLAN      : 0
```

```
    Report & Leave
     IGMP v1 Report               : 0
     IGMP v2 Report               : 0
     IGMP v3 Report               : 0
     IGMP v2 Leave                : 0
     Total                      : 0
     Dropped By Rate Limitation      : 0
     Dropped By Max Group Limitation  : 0
     Dropped By Group Filter         : 0
     Dropped By Multicast VLAN       : 0

Transmit Statistics
   Query
     IGMP v1 Query                : 0
     IGMP v2 Query                : 0
     IGMP v3 Query                : 8
     Total                      : 8

   Report & Leave
     IGMP v1 Report               : 0
     IGMP v2 Report               : 0
     IGMP v3 Report               : 0
     IGMP v2 Leave                : 0
     Total                      : 0

 Total Entries : 1

DGS-3200-10:4#
```

50-16 config igmp_snooping data_driven_learning

Purpose

To enable or disable data driven learning of an IGMP snooping group.

Format

config igmp_snooping data_driven_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}

Description

This command is used to enable or disable data driven learning of an IGMP snooping group. When data-driven learning is enabled for the VLAN, the switch receives the IP multicast traffic on this VLAN, and an IGMP snooping group is created. That is, the learning of an entry is not activated by IGMP membership registration, but activated by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care of the aging out of the entry. For a data-driven entry, the entry can be specified not to age out or to age out by the aging timer.

When data driven learning is enabled, the multicast filtering mode for all ports is ignored. This means multicast packets will be flooded. If a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. Thus, the aging out mechanism will follow the rules of an ordinary IGMP snooping entry.

Parameters

Parameters	Description
all	Specify all VLANs to be configured.
vlan_name	Specify the VLAN name to be configured.
vlianid	Specify a list of VLAN IDs to be configured.
state	Specify whether to enable or disable the data driven learning of an IGMP snooping group. This is enabled by default.
aged_out	Enable or disable the aging on the entry. This is disabled by default.
expiry_time	Specify the data driven group lifetime in seconds. This parameter is valid only when **aged_out** is enabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the data driven learning of an IGMP snooping group on the default VLAN:

```
DGS-3200-10:4#config igmp_snooping data_driven_learning vlan_name default state
enable aged_out enable expiry_time 260
Command: config igmp_snooping data_driven_learning vlan_name default state enabl
e aged_out enable expiry_time 260

Success.

DGS-3200-10:4#
```

50-17 config igmp_snooping data_driven_learning max_learned_entry

Purpose

To configure the maximum number of groups that can be learned by the data driven mechanism.

Format

config igmp_snooping data_driven_learning max_learned_entry <value 1-256>

Description

This command is used to configure the maximum number of groups that can be learned by the data driven mechanism. When the table is full, the system will stop learning new data-driven groups. Traffic for the new groups will be dropped.

Parameters

Parameters	Description
max_learned_entry	Specify the maximum number of groups that can be learned by the data driven mechanism. The default is 56.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the maximum number of groups that can be learned by the data driven mechanism:

```
DGS-3200-10:4#config igmp_snooping data_ driven_learning max_learned_entry 50
Command: config igmp_snooping data_ driven_learning max_learned_entry 50

Success.

DGS-3200-10:4#
```

50-18 clear igmp_snooping data_driven_group

Purpose

To delete the IGMP snooping group learned by the data driven mechanism.

Format

clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipaddr> | all]]

Description

This command is used to delete the IGMP snooping groups learned by the data driven mechanism.

Parameters

Parameters	Description
all	Delete all entries learned by the data driven mechanism.
vlan_name	Specify the VLAN name.
vlanid	Specify the VLAN ID.
ipaddress	Specify the IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete all the groups learned by the data-driven mechanism:

```
DGS-3200-10:4#clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.

DGS-3200-10:4#
```

50-19 show igmp_snooping forwarding

Purpose

To display the Switch's current IGMP snooping forwarding table.

Format

show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Description

This command is used to display the Switch's current IGMP snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group comes from in terms of specific sources. The packets come from the source VLAN. They will be forwarded to the forwarding ports.

Parameters

Parameters	Description
vlan	Specify a name of VLAN to be displayed.
vlanid	Specify a list of VLAN IDs to be displayed.

Restrictions

None.

Examples

To display all IGMP snooping forwarding entries located on the switch:

```
DGS-3200-10:4# show igmp_snooping forwarding
Command: show igmp_snooping forwarding

VLAN Name      : default
Source IP      : 10.90.90.114
Multicast Group: 225.0.0.0
Port Member    : 2,7

VLAN Name      : default
Source IP      : 10.90.90.10
Multicast Group: 225.0.0.1
Port Member    : 2,5

Total Entries : 2

DGS-3200-10:4#
```

50-20 show router_ports

Purpose

To display the currently configured router ports on the switch.

Format

show router_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic |f orbidden]}

Description

This command is used to display the currently configured router ports on the switch. If no parameter is specified, the system will display all currently configured router ports on the switch.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the router port resides.
vlanid	Specify a list of VIDs on which the router port resides.
static	Display router ports that have been statically configured.
dynamic	Display router ports that have been dynamically registered.
forbidden	Displays forbidden router ports that have been statically configured.

Restrictions

None.

Examples

To display the router ports:

```
DGS-3200-10:4#show router_ports all
Command: show router_ports all



VLAN Name                  : default
Static Router Port         : 1-10
Dynamic Router Port        :
Router IP                  :
Forbidden Router Port      :

Total Entries: 1



DGS-3200-10:4#
```

50-21 show igmp_snooping host

Purpose

To display the IGMP hosts that have joined groups on specific ports or specific VLANs.

Format

show igmp_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipaddr>]}

Description

This command is used to display the IGMP hosts that have joined groups on specific ports or specific VLANs.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the router port resides.
vlanid	Specify a list of VIDs on which the router port resides.
ports	Specify the list of ports to display the host information.
group	Specify the group to display the host information.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the host IP information:

```
DGS-3200-10:4# show igmp_snooping host vlan default
Command: show igmp_snooping host vlan default

 VLAN ID     Group             Port        IGMP
 --------  -----------------  ---------   ------------
 1           225.0.1.0             2             198.19.1.2
 1           225.0.1.0             2             198.19.1.3
 1           225.0.1.0             3             198.19.1.4
 1           225.0.1.2             2             198.19.1.3
 1           225.0.2.3             3             198.19.1.4
 1           225.0.3.4             3             198.19.1.5
 1           225.0.4.5             5             198.19.1.6
 1           225.0.5.6             5             198.19.1.7
 1           225.0.6.7             4             198.19.1.8
 1           225.0.7.8             4             198.19.1.9
 1           239.255.255.250     7             10.90.90.90

Total Entries : 11

DGS-3200-10:4#
```

50-22 clear igmp_snooping statistics counter

Purpose

To clear the IGMP snooping statistics counter.

Format

clear igmp_snooping statistics counter

Description

This command is used to clear the IGMP snooping statistics counter on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the IGMP snooping statistic counter:

```
DGS-3200-10:4# clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter

Success.

DGS-3200-10:4#
```

51 IGMP Authentication Command List

config igmp access_authentication ports [all | <portlist>] state [enable | disable]
show igmp access_authentication ports [all|<portlist>]

51-1 config igmp access_authentication ports

Purpose

To configure IGMP authentication port status.

Format

config igmp access_authentication ports [all | <portlist>] state [enable | disable]

Description

This command is used to enable or disable IGMP authentication for the specified port. When the command is enabled, and the switch receives an IGMP join request, the switch will send the access request to the RADIUS server to do the authentication.

Parameters

Parameters	Description
ports	Specify a range of ports to be configured.
state	Enable or disable the RADIUS authentication function on the specified ports.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable IGMP authentication for all ports:

```
DGS-3200-10:4#config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success.

DGS-3200-10:4#
```

51-2 show igmp access_authentication ports

Purpose

To display the current IGMP authentication configuration.

Format

show igmp access_authentication ports [all |<portlist>]

Description

This command is used to display the current IGMP authentication configuration.

Parameters

Parameters	Description
all	Specify to display all the ports.
portlist	Specify a range of ports to be displayed. When a port list is not specified, information for all ports will be displayed.

Restrictions

None.

Example

To display IGMP Access Control status for ports 1 to 4:

```
DGS-3200-10:4#show igmp access_authentication ports 1-4
Command: show igmp access_authentication ports 1-4

Port     State
-----    ---------
1        Enabled
2        Enabled
3        Enabled
4        Enabled

DGS-3200-10:4#
```

52 MLD Snooping Command List

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] { state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable]}
config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] |version <value 1-2>}
config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>
enable mld_snooping
disable mld_snooping
show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}
show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}
create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>
delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>
show mld_snooping static_group {[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipv6addr >}
config mld_snooping data_driven_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}
config mld_snooping data_driven_learning max_learned_entry <value 1-256>
clear mld_snooping data_driven_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipv6addr>| all]]
show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
clear mld_snooping statistics counter
show mld_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipv6addr>]}
config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

52-1 config mld_snooping

Purpose

To configure MLD snooping on the switch.

Format

config mld_snooping [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] { state [enable | disable] | fast_done [enable | disable] | report_suppression [enable | disable]}

Description

This command is used to configure MLD snooping on the switch.

Parameters

Parameters	Description
vlan_name	Specify a VLAN name to be configured.
vlanid	Specify a list of VLAN IDs to be configured
all	Specify to configure all VLANs.
state	**enable** or **disable** MLD snooping for the chosen VLAN.
fast_done	**enable** or **disable** the MLD snooping fast done function. If enabled, the membership is immediately removed when the system receives the MLD done message.
report_suppression	When MLD report suppression is enabled (the default), the Switch sends the first MLD report from all hosts for a group to all the multicast routers. The Switch does not send the remaining MLD reports for the group to the multicast routers. If the multicast router query includes requests only for MLDv1 reports, the Switch forwards only the first MLDv1 report from all hosts for a group to all the multicast routers. If the multicast router query also includes requests for MLDv2 reports, the Switch forwards all MLDv2 reports for a group to the multicast devices.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure MLD snooping:

```
DGS-3200-10:4#config mld_snooping vlan_name default state enable
Command: config mld_snooping vlan_name default state enable

Success.

DGS-3200-10:4#
```

52-2 config mld_snooping querier

Purpose

To configure the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, the permitted packet loss that guarantees MLD snooping.

Format

config mld_snooping querier [vlan_name <vlan_name 32> | vlanid <vlanid_list> | all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-7> | last_listener_query_interval <sec 1-25> | state [enable | disable] |version <value 1-2>}

Description

This command is used to configure the MLD snooping querier.

Parameters

Parameters	Description
vlan_name	The name of the VLAN for which the MLD snooping querier is to be configured.
vlanid	The VLAN IDs for which the MLD snooping querier is to be configured.
all	Specify **all** to indicate all VLANs to be configured.
query_interval	Specify the amount of time in seconds between general query transmissions. The default setting is 125 seconds.
max_reponse_time	The maximum time in seconds to wait for reports from listeners. The default setting is 10 seconds.
robustness_variable	Provide fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: • Group listener interval—Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • Other querier present interval—Amount of time that must pass before a

	multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • Last listener query count—Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to 2. You might want to increase this value if you expect a subnet to have a high loss.
last_listener_query_interval	The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group.
state	This allows the switch to be specified as an MLD Querier (sends MLD query packets) or a Non-Querier (does not send MLD query packets). Set to enable or disable.
version <value 1-2>	Specify the version of MLD packet that will be sent by this port. If a MLD packet received by the interface has a version higher than the specified version, this packet will be dropped.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MLD snooping querier:

```
DGS-3200-10:4#config mld_snooping querier vlan_name default query_interval 125
state enable
Command: config mld_snooping querier vlan_name default query_interval 125 state
enable

Success.

DGS-3200-10:4#
```

52-3 config mld_snooping mrouter_ports

Purpose

To configure ports as router ports.

Format

config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete]

<portlist>

Description

This command allows you to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.

Parameters

Parameters	Description
vlan	The name of the VLAN on which the router port resides.
vlanid	Specify a list of VLAN IDs to be configured.
add	Specify to add the router ports.
delete	Specify to delete the router ports.
portlist	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Example

To set up static router ports:

```
DGS-3200-10:4#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DGS-3200-10:4#
```

52-4 config mld_snooping mrouter_ports_forbidden

Purpose

To configure ports as forbidden router ports.

Format

config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vlanid_list>] [add | delete] <portlist>

Description

This command allows you to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.

Parameters

Parameters	Description
vlan	The name of the VLAN on which the router port resides.
vlanid	Specify a list of VLAN IDs to be configured.
add	Specify to add the router ports.
delete	Specify to add the router ports.
portlist	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure ports as forbidden router ports:

```
DGS-3200-10:4#config mld_snooping mrouter_ports_forbidden vlan default add 1-10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10


Success.


DGS-3200-10:4#
```

52-5 enable mld_snooping

Purpose

To enable MLD snooping on the switch.

Format

enable mld_snooping

Description

This command is used to enable MLD snooping on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable MLD snooping on the switch:

```
DGS-3200-10:4#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3200-10:4#
```

52-6 disable mld_snooping

Purpose

To disable MLD snooping on the switch.

Format

disable mld_snooping

Description

This command is used to disable MLD snooping on the switch. MLD snooping can be disabled only if IPv6 multicast routing is not being used. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a given IPv6 interface.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable MLD snooping on the switch:

```
DGS-3200-10:4#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3200-10:4#
```

52-7 show mld_snooping

Purpose

To display the current status of MLD snooping on the switch.

Format

show mld_snooping {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Description

This command is used to display the current MLD snooping configuration on the switch. If no parameter is specified, the system will display all current MLD snooping configurations.

Parameters

Parameters	Description
vlan	The name of the VLAN for which to view the MLD snooping configuration.
vlanid	The VLAN IDs for which to view the MLD snooping configuration.

Restrictions

None.

Example

To display MLD snooping:

```
DGS-3200-10:4#show mld_snooping
Command: show mld_snooping

 MLD Snooping Global State               : Enabled
 Data Driven Learning Max Entries        : 56

 VLAN Name                       : default
 Query Interval                  : 125
 Max Response Time               : 10
 Robustness Value                : 2
 Last Listener Query Interval  : 1
 Querier State                   : Disabled
 Querier Role                    : Non-Querier
 Querier IP                      : FE80::224:1FF:FE15:1C96
 Querier Expiry Time             : 0 secs
 State                           : Enabled
 Fast Done                       : Disabled
 Rate Limit                      : No Limitation
 Report Suppression              : Disabled
 Version                         : 2
 Data Driven Learning State    : Enabled
 Data Driven Learning Aged Out : Disabled
 Data Driven Group Expiry Time : 260

Total Entries: 1



DGS-3200-10:4#
```

52-8 show mld_snooping group

Purpose

To display the current MLD snooping group configuration on the switch.

Format

show mld_snooping group {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>] {<ipv6addr>}} {data_driven}

Description

This command is used to display the current MLD snooping group configuration on the switch. If no parameter is specified, the system will display all current MLD group snooping configuration of the Switch.

Parameters

Parameters	Description
vlan	The name of the VLAN for which to view MLD snooping group configuration information.
vlanid	The VLAN IDs for which to view MLD snooping group configuration information.
ports	Specify the list of port for which to view MLD snooping group information.
<ipv6addr>	Specify the group IPv6 address for which to view MLD snooping group information.
data_driven	Specify to display the data driven groups.

Restrictions

None.

Examples

To show the MLD snooping group:

```
DGS-3200-10:4#show mld_snooping group
Command: show mld_snooping

 Source/Group                   : 2001::2/FF1E::1
 VLAN Name/VID                  : default/1
 Member Ports                   : 8
 UP Time                        : 4
 Expiry Time                    : 256
 Filter Mode                    : INCLUDE

Total Entries: 1

DGS-3200-10:4#
```

52-9 show mld_snooping forwarding

Purpose

To display the current MLD snooping forwarding table.

Format

show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}

Description

This command is used to display the current MLD snooping forwarding table. It provides an easy way for users to check the list of ports that the multicast group that comes from specific sources will be forwarded to. The packet comes from the source VLAN will be forwarded to the forwarding VLAN. The MLD snooping further restricts the forwarding ports.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN for which you want to view MLD snooping forwarding table information.
vlanid	Specify the ID of the VLAN for which you want to view MLD snooping forwarding table information.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show all MLD snooping forwarding entries located on the Switch:

```
DGS-3200-10:4# show mld_snooping forwarding
Command: show mld_snooping forwarding

VLAN Name       : default
Source IP       : 2001::1
Multicast Group: FE1E::1
Port Member     : 2,7

VLAN Name       : default
Source IP       : 2001::2
Multicast Group: FF1E::1
Port Member     : 5

Total Entries : 2

DGS-3200-10:4#
```

52-10 show mld_snooping mrouter_ports

Purpose

To display the currently configured router ports on the switch.

Format

show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vlanid_list> | all] {[static | dynamic | forbidden]}

Description

This command is used to display the currently configured router ports on the switch. If no parameter is specified, the system will display all currently configured router ports on the switch.

Parameters

Parameters	Description
vlan	The name of the VLAN on which the router port resides.
vlanid	The VLAN IDs on which the router port resides.
all	Specify all VLANs on which the router port resides.
static	Displays router ports that have been statically configured.
dynamic	Displays router ports that have been dynamically configured.
forbidden	Displays forbidden router ports that have been statically configured.

Restrictions

None.

Example

To display router ports:

```
DGS-3200-10:4#show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all


VLAN Name                 : default
Static Router Port        : 1-10
Dynamic Router Port       :
Router IP                 :
Forbidden Router Port     :

 Total Entries: 1


DGS-3200-10:4#
```

52-11 create mld_snooping static_group

Purpose

To create an MLD snooping static group. Member ports can be added to the static group.

Format

create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Description

This command is used to create an MLD snooping multicast static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when MLD snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 MLD operation. The Reserved IP multicast addresses FF0x::/16 must be excluded from the configured group. The VLAN must be created first before a static group can be created.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipv6addr>	Specify the multicast group IPv6 address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an MLD snooping static group on vlan1, group FF1E::1:

```
DGS-3200-10:4# create mld_snooping static_group vlan vlan1 FF1E::1
Command: create mld_snooping static_group vlan vlan1 FF1E::1


Success.


DGS-3200-10:4#
```

52-12 config mld_snooping static_group

Purpose

To configure an MLD snooping static group on the switch.

Format

config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>

Description

This command is used to configure an MLD snooping static group on the switch. When a port is configured as a static member port, the MLD protocol will not operate on this port. Therefore, suppose that a port is a dynamic member port learned by MLD. If this port is configured as a static member later, then the MLD protocol will stop operating on this port. The MLD protocol will resume once this port is removed from static member ports. The static member port will only affect V1 MLD operation.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipv6addr>	Specify the multicast group IPv6 address.
add	Specify to add the member ports.
delete	Specify to delete the member ports.
<portlist>	Specify a range of ports to be configured.

Restrictions

Only Administrator-level users can issue this command.

Examples

To unset port range 9-10 from MLD snooping static member ports for group FF1E::1 on default VLAN:

```
DGS-3200-10:4#config mld_snooping static_group vlan default FF1E::1 add 9-10
Command: config mld_snooping static_group vlan default FF1E::1 add 9-10

Success.

DGS-3200-10:4#
```

52-13 delete mld_snooping static_group

Purpose

To delete an MLD snooping static group on the Switch.

Format

delete mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>

Description

This command is used to delete an MLD snooping static group on the Switch. The deletion of an MLD snooping static group will not affect the MLD snooping dynamic member ports for a group.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipv6addr>	Specify the multicast group IPv6 address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an MLD snooping static group from the default VLAN, group FF1E::1:

```
DGS-3200-10:4# delete mld_snooping static_group vlan default FF1E::1
Command: delete mld_snooping static_group vlan default FF1E::1

Success.

DGS-3200-10:4#
```

52-14 show mld_snooping static_group

Purpose

To display the MLD snooping multicast group static members.

Format

show mld_snooping static_group {[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipv6addr >}

Description

This command used to display the MLD snooping multicast group static members.

Parameters

Parameters	Description
vlan	Specify the name of the VLAN on which the static group resides.
vlanid	Specify the ID of the VLAN on which the static group resides.
<ipv6addr>	Specify the multicast group IPv6 address.

Restrictions

None.

Examples

To display all the MLD snooping static groups:

```
DGS-3200-10:4#show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name                      IP Address                  Static Member Ports
------------------------------  -------------------------  -------------------
1   /default                     FF1E::1                     9-10

 Total Entries : 1



DGS-3200-10:4#
```

52-15 config mld_snooping data_driven_learning

Purpose

To enable or disable the data-driven learning of an MLD snooping group.

Format

config mld_snooping data_driven_learning [all | vlan_name <vlan_name 32> | vlanid <vlanid_list>] {state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}

Description

This command is used to enable or disable the data-driven learning of an MLD snooping group. When data-driven learning is enabled for the VLAN, and the switch receives the IP multicast traffic, an MLD snooping group will be created on this VLAN. That is, the learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care the aging out of the entry. For a data-driven entry, the entry can be specified not to be aged out or to be aged out by the aged timer.

When the data driven learning is enabled, and the data driven table is not full, the multicast filtering mode for all ports is ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode.

Note that if a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. That is, the aging out mechanism will follow the ordinary MLD snooping entry.

Parameters

Parameters	Description
vlan_name	Specify the VLAN name to be configured.
vlanid	Specify the VLAN ID to be configured.
all	Specify that all VLANs are to be configured.
state	Specify to enable or disable the data driven learning of MLD snooping groups. By default, the state is enabled.
aged_out	Enable or disable the aging out of entries. By default, the state is disabled.
expiry_time	Specify the data driven group lifetime, in seconds. This parameter is valid only when **aged_out** is enabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
DGS-3200-10:4# config mld_snooping data_driven_learning vlan default state enable
Command: config mld_snooping data_driven_learning vlan default state enable

Success.

DGS-3200-10:4#
```

52-16 config mld_snooping data_driven_learning max_learned_entry

Purpose

To configure the maximum number of groups that can be learned by data driven.

Format

config mld_snooping data_driven_learning max_learned_entry <value 1-256>

Description

This command is used to configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop the learning of the new data-driven groups. Traffic for the new groups will be dropped.

Parameters

Parameters	Description
<value 1-256>	Specify the maximum number of groups that can be learned by data driven.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the maximum number of groups that can be learned by data driven:

```
DGS-3200-10:4# config mld_snooping data_driven_learning max_learned_entry 50
Command: config mld_snooping data_driven_learning max_learned_entry 50

Success.

DGS-3200-10:4#
```

52-17 clear mld_snooping data_driven_group

Purpose

To delete the MLD snooping groups learned by data driven.

Format

clear mld_snooping data_driven_group [all | [vlan_name <vlan_name 32> | vlanid <vlanid_list>] [<ipv6addr>| all]]

Description

This command is used to delete the MLD snooping groups learned by data driven.

Parameters

Parameters	Description
all	Specify all VLANs to which IGMP snooping groups will be deleted.
vlan_name	Specify the VLAN name.
vlanid	Specify the VLAN ID.
ipaddr	Specify the group's IP address learned by data driven.
all	Specify to clear all data driven groups of the specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete all the groups learned by data-driven:

```
DGS-3200-10:4# clear mld_snooping data_driven_group all
Command: clear mld_snooping data_driven_group all

Success.
```

```
DGS-3200-10:4#
```

52-18 show mld_snooping statistic counter

Purpose

To display the statistics counter for MLD protocol packets that are received by the switch since MLD snooping was enabled.

Format

show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]

Description

This command is used to display the statistics counter for MLD protocol packets that are received by the switch since MLD snooping was enabled.

Parameters

Parameters	Description
vlan	Specify a VLAN name to be displayed.
vlanid	Specify a list of VLANs to be displayed.
ports	Specify a list of ports to be displayed.

Restrictions

None.

Examples

To display the MLD snooping statistics counters on port 1:

```
DGS-3200-10:4# show mld_snooping statistic counter ports 1
Command: show mld_snooping statistic counter ports 1


Port #        : 1
-------------------------------------------------
Group Number    : 0


Receive Statistics
   Query
     MLD v1 Query               : 0
     MLD v2 Query               : 0
     Total                     : 0
```

```
     Dropped By Rate Limitation      : 0
    Dropped By Multicast VLAN       : 0

    Report & Done
     MLD v1 Report                 : 0
     MLD v2 Report                 : 0
     MLD v1 Done                  : 0
     Total                       : 0
     Dropped By Rate Limitation      : 0
     Dropped By Max Group Limitation  : 0
     Dropped By Group Filter         : 0
     Dropped By Multicast VLAN       : 0

Transmit Statistics
   Query
     MLD v1 Query                  : 0
     MLD v2 Query                  : 0
     Total                       : 0

    Report & Done
     MLD v1 Report                 : 0
     MLD v2 Report                 : 0
     MLD v1 Done                  : 0
     Total                       : 0

 Total Entries : 1

DGS-3200-10:4#
```

52-19 clear mld_snooping statistics counter

Purpose

To clear MLD snooping statistics counters.

Format

clear mld_snooping statistics counter

Description

This command is used to clear MLD snooping statistics counters.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear MLD snooping statistics counter.

```
DGS-3200-10:4# clear mld_snooping statistic counter
Command: clear mld_snooping statistic counter

Success.

DGS-3200-10:4#
```

52-20 show mld_snooping host

Purpose

To display the MLD host that has joined groups on specific port or specific VLAN.

Format

show mld_snooping host {[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist> | group <ipv6addr>]}

Description

This command is used to display the current host of a VLAN, port or group on the Switch. The hosts only take effect when fast leave is enabled. If no parameter is specified, it will display all hosts.

Parameters

Parameters	Description
vlan	Specify a VLAN name to be displayed.
vlanid	Specify a list of VLANs to be displayed.
ports	Specify a list of ports to be displayed.
group	Specify the group's IPv6 address to be displayed.

Restrictions

None.

Examples

To display the IP information.of hosts:

```
DGS-3200-10:4# show mld_snooping host vlan default
```

```
Command: show mld_snooping host vlan default

VLAN ID  :   1
Group    :   FF1E::1
Port     :   2
Host     :   2001::1

VLAN ID  :   1
Group    :   FF1E::2
Port     :   3
Host     :   2001::1

VLAN ID  :   1
Group    :   FF1E::3
Port     :   4
Host     :   2001::1

VLAN ID  :   1
Group    :   FF1E::1
Port     :   5
Host     :   2001::2

Total Entries : 4

DGS-3200-10:4#
```

To display the host's IP information for the group "FF1E::1":

```
DGS-3200-10:4# show mld_snooping host group FF1E::1
Command: show mld_snooping host group FF1E::1

VLAN ID  :   1
Group    :   FF1E::1
Port     :   2
Host     :   2001::1

VLAN ID  :   1
Group    :   FF1E::1
Port     :   5
```

```
Host      :   2001::2


Total Entries : 2


DGS-3200-10:4#
```

52-21 config mld_snooping rate_limit

Purpose

To configure the rate limit of MLD control packets that are allowed by each port or VLAN.

Format

config mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>] [<value 1-1000> | no_limit]

Description

This command is used to configure the rate limit of MLD control packets that are allowed by each port or VLAN.

Parameters

Parameters	Description
ports	Specify a list of ports to be configured.
vlanid	Specify a list of VLANs to be configured.
<value 1-1000>	Configure the rate limit of MLD control packets that the Switch can process on a specific port or VLAN. The rate is specified in packet per second. The packets that exceed the limited rate will be dropped.
no_limit	Specify to have unlimited rate of MLD control packets.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the MLD snooping per port rate limit:

```
DGS-3200-10:4# config mld_snooping ports 1 rate_limit 100
Command: config mld_snooping ports 1 rate_limit 100


Success.


DGS-3200-10:4#
```

52-22 show mld_snooping rate_limit

Purpose

To display the rate limit of MLD control packets that are allowed by each port.

Format

show mld_snooping rate_limit [ports <portlist> | vlanid <vlanid_list>]

Description

This command is used to display the rate limit of MLD control packets that are allowed by each port.

Parameters

Parameters	Description
ports	Specify a list of ports to be displayed.
vlanid	Specify a list of VLANs to be displayed.

Restrictions

None.

Examples

To display the mld_snooping per port rate_limit:

```
DGS-3200-10:4# show mld_snooping rate_limit ports 1-5
Command: show mld_snooping rate_limit ports 1-5

Port       Rate Limit
--------   -----------
 1         No Limit
 2         100
 3         No Limit
 4         No Limit
 5         No Limit

Total Entries: 5

DGS-3200-10:4#
```

53 Limited Multicast IP Address Command List

create mcast_filter_profile {profile_id <value 1-24> profile_name <name 32>}
config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}
delete mcast_filter_profile [profile_id [<value 1-24> | all] | profile_name <name 32>]
show mcast_filter_profile {[profile_id <value 1-24> | profile_name <name 32>]}
config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>]{[add | delete] [profile_id <value 1-24> | profile_name <name 32>] | access [permit | deny]}
config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {max_group [<value 1-1024> | infinite] | action [drop | replace]}
show max_mcast_group [ports <portlist>|vlanid <vlanid_list>]
show limited_multicast_addr [ports <portlist>|vlanid <vlanid_list>]

53-1 create mcast_filter_profile

Purpose

To create a multicast address profile.

Format

create mcast_filter_profile {profile_id <value 1-24> profile_name <name 32>}

Description

This command is used to create a multicast address profile.

Parameters

Parameters	Description
profile_id	Specify the ID of the profile.
profile_name	Provide a meaningful description for the profile.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a multicast address profile named MOD:

```
DGS-3200-10:4# create mcast_filter_profile profile_id 2 profile_name MOD
Command: create mcast_filter_profile profile_id 2 profile_name MOD

Success.

DGS-3200-10:4#
```

53-2 config mcast_filter_profile

Purpose

To add or delete a range of multicast addresses to the profile.

Format

config mcast_filter_profile [profile_id <value 1-24> | profile_name <name 32>] {profile_name <name 32> | [add | delete] <mcast_address_list>}

Description

This command is used to add or delete a range of multicast IP addresses.

Parameters

Parameters	Description
profile_id	The ID of the profile.
profile_name	Provide a description for the profile.
mcast_address_list	List of the multicast addresses to be put in the profile. Specifiy either a single multicast IP address or a range of multicast addresses using a hyphen.
add	Specify to add a list of multicast addresses.
delete	Specify to delete a list of multicast addresses.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a range of multicast addresses to a profile:

```
DGS-3200-10:4# config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1 - 225.1.1.1

Success.

DGS-3200-10:4#
```

53-3 delete mcast_filter_profile

Purpose

To delete a multicast address profile.

Format

delete mcast_filter_profile [profile_id [<value 1-24> | all] | profile_name <name 32>]

Description

This command is used to delete a multicast address profile.

Parameters

Parameters	Description
profile_id	Specify the ID of the profile. Specify all to delte all multicast address profiles.
profile_name	Specify a profile based on the profile name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a multicast profile with a profile ID of 3:

```
DGS-3200-10:4# delete mcast_filter_profile profile_id 3
Command: delete mcast_filter_profile profile_id 3

Success.

DGS-3200-10:4#
```

To delete a multicast profile with a profile named MOD:

```
DGS-3200-10:4# delete mcast_filter_profile profile_name MOD
Command: delete mcast_filter_profile profile_name MOD

Success.

DGS-3200-10:4#
```

53-4 show mcast_filter_profile

Purpose

To display defined multicast address profiles.

Format

show mcast_filter_profile {[profile_id <value 1-24> | profile_name <name 32>]}

Description

This command is used to display defined multicast address profiles.

Parameters

Parameters	Description
profile_id	The ID of the profile.
profile_name	The name of the profile.

Restrictions

None.

Examples

To display defined multicast address profiles:

```
DGS-3200-10:4#show mcast_filter_profile
Command: show mcast_filter_profile

Profile ID     Name             Multicast Addresses
----------    -----------      ----------------------------
1             MOD              234.1.1.1 - 238.244.244.244
                               234.1.1.1 - 238.244.244.244
2             customer          224.19.62.34 - 224.19.162.200

Total Entries : 2

DGS-3200-10:4#
```

53-5 config limited_multicast_addr

Purpose

To configure the multicast address filtering function on a port or VLAN.

Format

config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>]{[add | delete] [profile_id <value 1-24> | profile_name <name 32>] | access [permit | deny]}

Description

This command is used to configure the multicast address filtering function on a port or VLAN. When there is no profile specified with a port or VLAN, the limited function is not effective. When the function is configured on a port, it limits the multicast group operated by the IGMP or MLD snooping function and the layer 3 functions. When this function is configured on a VLAN, the multicast group is limited to only operate the IGMP or MLD layer 3 functions.

Parameters

Parameters	Description
ports	Specify the range of ports to configure the multicast address filtering function.
vlanid	Specify the VLAN ID of the VLAN that the multicast address filtering function will be configured on.
add	Specify to add a multicast address profile to a port.
delete	Specify to delete a multicast address profile to a port.
profile_id	Specify a profile ID to be added to or deleted from the port.
profile_name	Specify a profile name to be added to or deleted from the port.
access	Specify whether the access is permit or deny.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add multicast address profile 2 to ports 1 and 3:

```
DGS-3200-10:4# config limited_multicast_addr ports 1,3  add profile_id 2
Command: config limited_multicast_addr ports 1,3  add profile_id 2

Success.

DGS-3200-10:4#
```

53-6 config max_mcast_group

Purpose

To configure the maximum number of multicast groups that a port can join.

Format

config max_mcast_group [ports <portlist> | vlanid <vlanid_list>] {max_group [<value 1-1024> | infinite] | action [drop | replace]}

Description

This command is used to configure the maximum number of multicast groups that a port can join.

Parameters

Parameters	Description
ports	Specify a range of ports to configure the maximum multicast group.
vlanid	Specify the VLAN ID to configure the maximum multicast group.
max_group	Specify the maximum number of the multicast groups.
infinite	The maximum number of multicast groups per port or VLAN is not limited by the Switch.
action	Specify the action for handling newly learned groups when the register is full. **drop** - The new group will be dropped. **replace** - The new group will replace the oldest group in the register table.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the maximum number of multicast group that ports 1 and 3 can join to 100:

```
DGS-3200-10:4# config max_mcast_group ports 1, 3 max_group 100
Command: config max_mcast_group ports 1, 3 max_group 100

Success.

DGS-3200-10:4#
```

53-7 show max_mcast_group

Purpose

To display the maximum number of multicast groups that a port can join.

Format

show max_mcast_group [ports <portlist>|vlanid <vlanid_list>]

Description

This command is used to display the maximum number of multicast groups that a port can join.

Parameters

Parameters	Description
ports	Specify a range of ports to display the maximum multicast group.
vlanid	Specify the VLAN ID to display the maximum multicast group.

Restrictions

None.

Examples

To display the maximum number of multicast groups that port 1 can join:

```
DGS-3200-10:4# show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Port     Max Multicast Group Number   Action
------   ---------------------------  ---------
1        Infinite                      Drop

Total Entries: 1

DGS-3200-10:4#
```

53-8 show limited_multicast_addr

Purpose

To show the limited IP multicast address range for each port or VLAN.

Format

show limited_multicast_addr [ports <portlist>|vlanid <vlanid_list>]

Description

This command is used to show the limited IP multicast address range for each port or VLAN.

Parameters

Parameters	Description
ports	Specify the range of ports to display the multicast address filtering function information.
vlanid	Specify the VLAN ID to display the multicast address filtering function information.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the limited multicast address range on VLAN 1:

```
DGS-3200-10:4# show limited_multicast_addr vlanid 1
Command: show limited_multicast_addr vlanid 1

VLAN   : 1
Access  : Deny

Profile ID     Name              Multicast Addresses
-----------   -----------         ----------------------------
1           customer           224.19.62.34 – 224.19.162.200

DGS-3200-10:4#
```

To display the limited multicast address range on ports 1 and 3:

```
DGS-3200-10:4# show limited_multicast_addr ports 1,3
Command: show limited_multicast_addr ports 1,3

Port   : 1
Access  : Deny

Profile ID     Name              Multicast Addresses
-----------   -----------         ----------------------------
1           customer           224.19.62.34 – 224.19.162.200


Port   : 3
Access  : Deny

Profile ID     Name              Multicast Addresses
-----------   ----------------     ----------------------------
1           customer           224.19.62.34 – 224.19.162.200

DGS-3200-10:4#
```

54 IGMP Snooping Multicast VLAN (ISM) Command List

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> |tag_member_port <portlist>]| state [enable|disable] |replace_source_ip <ipaddr>}
create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>
config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>
delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> |all]
show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}
config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>
show igmp_snooping multicast_vlan_group {< vlan_name 32>}
delete igmp_snooping multicast_vlan <vlan_name 32>
enable igmp_snooping multicast_vlan
disable igmp_snooping multicast_vlan
show igmp_snooping multicast_vlan {<vlan_name 32>}
config igmp_snooping multicast_vlan forward_unmatched [disable | enable]

54-1 create igmp_snooping multicast_vlan

Purpose

To create an IGMP snooping multicast VLAN.

Format

create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>

Description

This command is used to create a multicast VLAN. Multiple multicast VLANs can be configured. The ISM VLANs being created can not exist in the 1Q VLAN database. Multiple ISM VLANs can be created. The ISM VLAN snooping function co-exists with the 1Q VLAN snooping function..

Parameters

Parameters	Description
vlan_name	The name of the multicast VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters.
vlanid	The VLAN ID of the multicast VLAN to be created. The range is from 2 to 4094.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IGMP snooping multicast VLAN called “mv1 2”:

```
DGS-3200-10:4# create igmp_snooping multicast_vlan mv1 2
Command: create igmp_snooping multicast_vlan mv1 2

Success.

DGS-3200-10:4#
```

54-2 config igmp_snooping multicast_vlan

Purpose

To configure the parameters of a specific IGMP snooping multicast VLAN.

Format

config igmp_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> |tag_member_port <portlist>]| state [enable|disable] |replace_source_ip <ipaddr>}

Description

This command is used to add member ports and add source ports to a port list. The member port will automatically become an untagged member of the multicast VLAN, and the source port will automatically become a tagged member of the multicast VLAN. The member port list and source port list can not overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. The multicast VLAN must be created first, before configuration.

Parameters

Parameters	Description
vlan_name	The name of the multicast VLAN to be configured. Each multicast VLAN is given a name that can be up to 32 characters.
member_port	A range of member ports to add to the multicast VLAN. They will become the untagged member ports of the ISM VLAN.
tag_member_port	Specify the tagged member port of the ISM VLAN.
source_port	A range of member ports to add to the multicast VLAN.
state	Enable or disable multicast VLAN for the chosen VLAN.
replace_source_ip	With the IGMP snooping function, the IGMP report packet sent by the host

	will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to be replaced by this IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add port 1 as a member of the “v1” IGMP snooping multicast VLAN:

```
DGS-3200-10:4# config igmp_snooping multicast_vlan ism1 add member_port 1,3 state
enable replace_source_ip 10.0.0.1
Command: config igmp_snooping multicast_vlan ism1 add member_port 1,3 state enable
replace_source_ip 10.0.0.1

Success.

DGS-3200-10:4#
```

54-3 create igmp_snooping multicast_vlan_group_profile

Purpose

To create a multicast group profile.

Format

create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>

Description

This command is used to create a multicast group profile. The profile name for IGMP snooping must be unique.

Parameters

Parameters	Description
<profile_name 1-32>	Specify the multicast VLAN profile name. The maximum length is 32 characters.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create an IGMP snooping multicast group profile with the name “Knicks”:

```
DGS-3200-10:4# create igmp_snooping multicast_vlan_group_profile Knicks
Command: create igmp_snooping multicast_vlan_group_profile Knicks

Success.

DGS-3200-10:4#
```

54-4 config igmp_snooping multicast_vlan_group_profile

Purpose

To configure an IGMP snooping multicast group profile on the switch and to add or delete multicast addresses for a profile.

Format

config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>

Description

This command is used to configure an IGMP snooping multicast group profile on the switch and to add or delete multicast addresses for a profile.

Parameters

Parameters	Description
<profile_name 1-32>	Specify the multicast VLAN profile name. The maximum length is 32 characters.
add	Specify to add a multicast address list to this multicast VLAN profile.
delete	Specify to delete a multicast address list from this multicast VLAN profile.
<mcast_address_list>	Specify a multicast address list. This can be a continuous single multicast address, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, a multicast address range, such as 225.1.1.1-225.2.2.2, or both types, such as 225.1.1.1, 225.1.1.18-225.1.1.20.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add the single multicast address 225.1.1.1 and multicast range 225.1.1.10-225.1.1.20 to the IGMP snooping multicast VLAN profile named “Knicks”:

```
DGS-3200-10:4#config igmp_snooping multicast_vlan_group_profile Knicks add 225.1.1.1,
225.1.1.10-225.1.1.20
Command: config igmp_snooping multicast_vlan_group_profile Knicks add 225.1.1.1,
225.1.1.10-225.1.1.20

Success.

DGS-3200-10:4#
```

54-5 delete igmp_snooping multicast_vlan_group_profile

Purpose

To delete an existing IGMP snooping multicast group profile on the switch.

Format

delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> |all]

Description

This command is used to delete an existing IGMP snooping multicast group profile on the switch. Specify a profile name to delete it.

Parameters

Parameters	Description
<profile_name 1-32>	Specify the multicast VLAN profile name. The maximum length is 32 characters.
all	Specify to delete all the profiles.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IGMP snooping multicast group profile named “Knicks”:

```
DGS-3200-10:4# delete igmp_snooping multicast_vlan_group_profile profile_name Knicks
Command: delete igmp_snooping multicast_vlan_group_profile profile_name Knicks

Success.

DGS-3200-10:4#
```

54-6 show igmp_snooping multicast_vlan_group_profile

Purpose

To display an IGMP snooping multicast group profile.

Format

show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}

Description

This command is used to display an IGMP snooping multicast group profile.

Parameters

Parameters	Description
<profile_name 1-32>	Specify the multicast VLAN profile name. The maximum length is 32 characters.

Restrictions

None.

Examples

To display all IGMP snooping multicast VLAN profiles:

```
DGS-3200-10:4# show igmp_snooping multicast_vlan_group_profile
Command: show igmp_snooping multicast_vlan_group_profile

Profile Name               Multicast Addresses
-----------------------  --------------------------------
Knicks                   234.1.1.1 - 238.244.244.244
                         239.1.1.1 - 239.2.2.2
customer                 224.19.62.34 - 224.19.162.200

Total Entries : 2

DGS-3200-10:4#
```

54-7 config igmp_snooping multicast_vlan_group

Purpose

To configure the multicast group which will be learned with the specific multicast VLAN.

Format

config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>

Description

This command is used to configure the multicast group which will be learned with the specific multicast VLAN. There are two cases that need to be considered. For the first case, suppose that a multicast group is not configured and multicast VLANs do not have overlapped member ports. That means the join packets received by the member port will only be learned with the multicast VLAN that this port belongs to. If not, which is the second case, the join packet will be learned with the multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet can not be classified into any multicast VLAN that this port belongs to, then the join packet will be learned with the natural VLAN of the packet.

Please note that the same profile can not overlap different multicast VLANs. Multiple profiles can be added to a multicast VLAN, however.

Parameters

Parameters	Description
vlan_name	The name of the multicast VLAN to be configured. Each multicast VLAN is given a name that can be up to 32 characters.
add	Used to associate a profile to a multicast VLAN.
delete	Used to de-associate a profile from a multicast VLAN.
profile_name	Specifies the multicast vlan profile name. The maximum length is 32 characters.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a profile to a multicast VLAN:

```
DGS-3200-10:4# config igmp_snooping multicast_vlan_group v1 add profile_name
channel_1
Command: config igmp_snooping multicast_vlan_group v1 add profile_name channel_1
Success.

DGS-3200-10:4#
```

54-8 show igmp_snooping multicast_vlan_group

Purpose

To display group profile information for a specific multicast VLAN.

Format

show igmp_snooping multicast_vlan_group {< vlan_name 32>}

Description

This command is used to display group profile information for a specific multicast VLAN.

Parameters

Parameters	Description
<vlan_name 32>	Specify the name of the group profile's multicast VLAN to be displayed.

Restrictions

None.

Examples

To display all IGMP snooping multicast VLANs'group profile information:

```
DGS-3200-10:4# show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group


VLAN Name                       VLAN ID  Multicast Group Profiles
-------------------------  -------  ---------------------------------
Mv1                              20          channel_1

DGS-3200-10:4#
```

54-9 delete igmp_snooping multicast_vlan

Purpose

To delete a multicast VLAN.

Format

delete igmp_snooping multicast_vlan <vlan_name 32>

Description

This command is used to delete a multicast VLAN.

Parameters

Parameters	Description
vlan_name	The name of the multicast VLAN to be deleted.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IGMP snooping multicast VLAN:

```
DGS-3200-10:4# delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicast_vlan v1

Success.

DGS-3200-10:4#
```

54-10 enable igmp_snooping multicast_vlan

Purpose

To enable the multicast VLAN function.

Format

enable igmp_snooping multicast_vlan

Description

This command is used to control the multicast VLAN function. The command enable igmp_snooping controls the ordinary IGMP snooping function. By default, the multicast VLAN is disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable IGMP snooping multicast VLAN:

```
DGS-3200-10:4# enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DGS-3200-10:4#
```

54-11 disable igmp_snooping multicast_vlan

Purpose

To disable the multicast VLAN function.

Format

disable igmp_snooping multicast_vlan

Description

This command is used to disable multicast VLAN.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable IGMP snooping multicast VLAN:

```
DGS-3200-10:4# disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan

Success.

DGS-3200-10:4#
```

54-12 show igmp_snooping multicast_vlan

Purpose

To display multicast VLAN information.

Format

show igmp_snooping multicast_vlan {<vlan_name 32>}

Description

This command is used to display multicast VLAN information.

Parameters

Parameters	Description
vlan_name	The name of the multicast VLAN to be shown.

Restrictions

None.

Examples

To display all IGMP snooping multicast VLANs:

```
DGS-3200-10:4# show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State        : Disabled
IGMP Multicast VLAN Forward Unmatched   : Disabled

VLAN Name                : mv1
VID                      : 2

Member(Untagged) Ports   : 1,3
Tagged Member Ports      : 2
Source Ports             : 4
Status                   : Enabled
Replace Source IP        : 10.1.1.100

DGS-3200-10:4#
```

54-13 config igmp_snooping multicast_vlan forward_unmatched

Purpose

To configure the forwarding mode for IGMP snooping multicast VLAN unmatched packets.

Format

config igmp_snooping multicast_vlan forward_unmatched [disable | enable]

Description

This command is used to configure the forwarding mode for IGMP snooping multicast VLAN unmatched packets. When the switch receives an IGMP snooping packet, it will match the packet against the multicast profile to determine which multicast VLAN to associate with. If the packet does not match all profiles, the packet will be forwarded or dropped based on this setting. By default, the packet will be dropped.

Parameters

Parameters	Description
disable	The packet will be dropped.
enable	The packet will be flooded on the VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the forwarding mode for IGMP snooping multicast VLAN unmatched packets:

```
DGS-3200-10:4# config igmp_snooping multicast_vlan forward_unmatched enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3200-10:4#
```

VIII. Security

The Security section includes the following chapters: 802.1X, Access Authentication Control, SSL, SSH, IP-MAC-Port Binding (IMPB), Web-based Access Control, MAC-based Access Control, JWAC, Multiple Authentication, Filter, ARP Spoofing Prevention, and CPU Filter.

55 802.1X Command List

enable 802.1x
disable 802.1x
create 802.1x user <username 15>
delete 802.1x user <username 15>
show 802.1x user
config 802.1x auth_protocol [local|radius_eap]
config 802.1x fwd_pdu ports [<portlist>|all] [enable|disable]
config 802.1x fwd_pdu system [enable|disable]
config 802.1x authorization attributes radius [enable | disable]
show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}
config 802.1x capability ports [<portlist>|all] [authenticator|none]
config 802.1x max_users [<value 1-448> |no_limit]
config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}
config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]
create 802.1x guest_vlan {<vlan_name 32>}
delete 802.1x guest_vlan {<vlan_name 32>}
config 802.1x guest_vlan ports [<portlist>|all] state [enable | disable]
show 802.1x guest_vlan
config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port<udp_port_number 1-65535 > | acct_port <udp_port_number 1-65535 > | timeout<sec 1-255> | retransmit<int 1-20>}]
config radius delete <server_index 1-3>

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port[<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}
show radius
show auth_statistics {ports <portlist>}
show auth_diagnostics {ports <portlist>}
show auth_session_statistics {ports <portlist>}
show auth_client
show acct_client
config accounting service [network|shell|system] state [enable|disable]
show accounting service

55-1 enable 802.1x

Purpose

To enable the 802.1x function.

Format

enable 802.1x

Description

This command is used to enable the 802.1x function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the 802.1x function:

```
DGS-3200-10:4#enable 802.1x
Command: enable 802.1x

Success.

DGS-3200-10:4#
```

55-2 disable 802.1x

Purpose

To disable the 802.1x function.

Format

disable 802.1x

Description

This command is used to disable the 802.1x function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the 802.1x function:

```
DGS-3200-10:4#disable 802.1x
Command: disable 802.1x

Success.

DGS-3200-10:4#
```

55-3 create 802.1x user

Purpose

To create the 802.1x user.

Format

create 802.1x user <username 15>

Description

This command is used to create an 802.1x user.

Parameters

Parameters	Description
username	Specify adding a user name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a user named “ctsnow”.

```
DGS-3200-10:4#create 802.1x user ctsnow
Command: create 802.1x user ctsnow

Enter a case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DGS-3200-10:4#
```

55-4 delete 802.1x user

Purpose

To delete an 802.1x user.

Format

delete 802.1x user <username 15>

Description

This command is used to delete a specified user.

Parameters

Parameters	Description
username	Specify deleting a user name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete the user named “Tiberius”.

```
DGS-3200-10:4#delete 802.1x user Tiberius
Command: delete 802.1x user Tiberius

Success.

DGS-3200-10:4#
```

55-5 show 802.1x user

Purpose

To display the 802.1x user.

Format

show 802.1x user

Description

This command is used to display 802.1x user account information.

Parameters

None.

Restrictions

None.

Examples

To display 802.1x user information:

```
DGS-3200-10:4#show 802.1x user
Command: show 802.1x user

Current Accounts:
UserName          Password
---------------   ------------
ctsnow            gallinari

Total Entries : 1

DGS-3200-10:4#
```

55-6 config 802.1x auth_protocol

Purpose

To configure the 802.1x authentication protocol.

Format

config 802.1x auth_protocol [local|radius_eap]

Description

This command is used to configure the 802.1x authentication protocol.

Parameters

Parameters	Description
local	Specify the authentication protocol as local.
radius_eap	Specify the authentication protocol as RADIUS EAP

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure 802.1x RADIUS EAP:

```
DGS-3200-10:4#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.

DGS-3200-10:4#
```

55-7 config 802.1x fwd_pdu ports

Purpose

To configure the 802.1X PDU forwarding state on specific ports of the switch.

Format

config 802.1x fwd_pdu ports [<portlist>|all] [enable|disable]

Description

This command is used to configure the 802.1X PDU forwarding state on specific ports of the switch.

Parameters

Parameters	Description
ports	Specify the range of ports to be configured.
all	Specify all ports to be configured.
enable	Enable the 802.1X PDU forwarding state.
disable	Disable the 802.1X PDU forwarding state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 802.1X PDU forwarding state on ports 1 to 2:

```
DGS-3200-10:4# config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu ports 1-2 enable

Success.

DGS-3200-10:4#
```

55-8 config 802.1x fwd_pdu system

Purpose

To configure the forwarding of EAPOL PDUs when 802.1X is disabled.

Format

config 802.1x fwd_pdu system [enable|disable]

Description

This is a global setting to control the forwarding of EAPOL PDUs. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports which have 802.1X fwd_pdu enabled on and 802.1X is disabled (globally or just for the port). The default state is disabled.

Parameters

Parameters	Description
enable	Enable the forwarding of EAPOL PDUs.
disable	Disable the forwarding of EAPOL PDUs.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the 802.1X EAPOL PDU forward state:

```
DGS-3200-10:4# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3200-10:4#
```

55-9 config 802.1x authorization attributes

Purpose

To enable or disable the acceptation of an authorized configuration.

Format

config 802.1x authorization attributes radius [enable | disable]

Description

This command is used to enable or disable the acceptation of an authorized configuration. (To configure that attributes, regarding VLAN, 802.1p, ACL and Ingress/Egress Bandwidth, please refer to the Appendix section at the end of this document.)

Parameters

Parameters	Description
radius	If specified to **enable**, the authorization attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is **enabled**. The default state is **enabled**.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 802.1X state of acceptation of an authorized configuration:

```
DGS-3200-10:4#config 802.1x authorization attributes radius enable
Command: config 802.1x authorization attributes radius enable

Success.

DGS-3200-10:4#
```

55-10 show 802.1x

Purpose

To display the 802.1x state or configurations.

Format

show 802.1x {[auth_state | auth_configuration] ports {<portlist>}}

Description

This command is used to display the 802.1x state or configurations.

Parameters

Parameters	Description
auth_state	Use to display 802.1x authentication state machine of some or all ports
auth_configuration	Use to display 802.1x configurations of some or all ports.
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display the 802.1x global configuration:

```
DGS-3200-10:4#show 802.1x
Command: show 802.1x

802.1X                    : Enabled
Authentication Protocol : RADIUS_EAP
Forward EAPOL PDU         : Disabled
Max User                  : 448
RADIUS Authorization      : Enabled

DGS-3200-10:4#
```

To display the 802.1x configuration for ports 1-5:

```
DGS-3200-10:4# show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

Status:  A – Authorized; U – Unauthorized; (P): Port-Based 802.1X Pri: Priority
Port    MAC Address        Auth   PAE State     Backend     Status  VID   Pri
                           VID                  State
----- ------------------- ------- ------------- ---------- ------ ----- -----
1    00-00-00-00-00-01     10      Authenticated  Idle        A      4004   3
1    00-00-00-00-00-02     10      Authenticated  Idle        A      1234   -
1    00-00-00-00-00-04     30      Authenticating Response    U       -     -
2    -                (P)  -       Authenticating  Request     U       -     -
3    -                (P)  -       Connecting      Idle        U       -     -
4    -                (P)  -       Held            Fail        U       -     -
5    -                (P)  -       Authenticated   Idle        A      100    -
Total Authenticating Hosts: 3
Total Authenticated Hosts : 3

DGS-3200-10:4#
```

To display the 802.1x configuration for port 1:

```
DGS-3200-10:4# show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

Port Number    : 1
Capability     : None
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : Auto
QuietPeriod    : 60    sec
TxPeriod       : 30    sec
SuppTimeout    : 30    sec
ServerTimeout  : 30    sec
MaxReq         : 2     times
ReAuthPeriod   : 3600  sec
ReAuthenticate : Disabled
Forward EAPOL PDU On Port : Disabled
Max User On Port : 16

DGS-3200-10:4#
```

55-11 config 802.1x capability ports

Purpose

To configure port capability.

Format

config 802.1x capability ports [<portlist>|all] [authenticator|none]

Description

This command is used to configure port capability.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.
all	All ports.
authenticator	The port that wishes to enforce authentication before allowing access to services that are accessible via that port adopts the authenticator role.
none	Allow the flow of PDUs via the port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port capability:

```
DGS-3200-10:4#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3200-10:4#
```

55-12 config 802.1x max_users

Purpose

To configure the maximum number of users that can be learned via 802.1X authentication.

Format

config 802.1x max_users [<value 1-448> |no_limit]

Description

The setting is a global limitation on the maximum number of users that can be learned via 802.1X authentication. In addition to the global limitation, the maximum number of users per port is also limited. It is specified by the config 802.1x auth_parameter command.

Parameters

Parameters	Description
<value 1-448>	Specify the maximum number of users.
no_limit	Specify an unlimited number of users.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 820.1X maximum numbers of the system:

```
DGS-3200-10:4# config 802.1x max_users 2
Command: config 802.1x max_users 2

Success.

DGS-3200-10:4#
```

55-13 config 802.1x auth_parameter ports

Purpose

To configure the parameters that control the operation of the authenticator associated with a port.

Format

config 802.1x auth_parameter ports [<portlist> | all] [default | {direction [both] | port_control [force_unauth | auto | force_auth] | quiet_period <sec 0-65535> | tx_period <sec 1-65535> | supp_timeout <sec 1-65535> | server_timeout <sec 1-65535> | max_req <value 1-10> | reauth_period <sec 1-65535> | max_users [<value 1-448> | no_limit] | enable_reauth [enable | disable]}]

Description

This command is used to configure the parameters that control the operation of the authenticator associated with a port.

Parameters

Parameters	Description	
portlist	Specify a range of ports to be configured.	
all	All ports.	
default	Set all parameter to be default value.	
direction	Set the direction of access control.	
	both	For bidirectional access control.
port_control	Force a specific port to be unconditionally authorized or unauthorized by setting the parameter of **port_control** to be **force_auth** or **force_unauth**. Besides, the controlled port will reflect the outcome of authentication if **port_control** is **auto**.	
	force_auth	The port transmits and receives normal traffic without 802.1X-based authentication of the client.
	auto	The port begins in the unauthorized state, and relays authentication messages between the client and the authentication server.
	force_unauth	The port will remain in the unauthorized state, ignoring all attempts by the client to authenticate.
quiet_period	The initialization value of the quietWhile timer. The default value is 60 s and can be any value from 0 to 65535.	
tx_period	The initialization value of the txWhen timer. The default value is 30 s and can be any value from 1 to 65535.	

supp_timeout	The initialization value of the aWhile timer when timing out the supplicant. Its default value is 30 s and can be any value from 1 to 65535.
server_timeout	The initialization value of the aWhile timer when timing out the authentication server. Its default value is 30 and can be any value from 1 to 65535.
max_req	The maximum number of times that the authentication PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is 2 and can be any number from 1 to 10.
reauth_period	Its a non-zero number of seconds, which is used to be the re-authentication timer. The default value is 3600.
max_users	Specify the maximum number of users between 1 and 448. Specify **no_limit** to have an unlimited number of users.
enable_reauth	Enable or disable the re-authentication mechanism for a specific port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the parameters that control the operation of the authenticator associated with a port:

```
DGS-3200-10:4# config 802.1x auth_parameter ports 1-10 direction both
Command: config 802.1x auth_parameter ports 1-10 direction both

Success.

DGS-3200-10:4#
```

55-14 config 802.1x init

Purpose

To initialize the authentication state machine of some or all ports.

Format

config 802.1x init [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

Description

This command is used to initialize the authentication state machine of some or all.

Parameters

Parameters	Description
port_based	Use to configure authentication in port-based mode.
mac_based	To configure authentication in host-based 802.1X mode, the user first

	must enable the 802.1X MAC-based setting.
portlist	Specify a range of ports to be configured.
all	All ports.
mac_address	The MAC address of the host.

Restrictions

Only Administrator-level users can issue this command.

Examples

To initialize the authentication state machine of some or all:

```
DGS-3200-10:4# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3200-10:4#
```

55-15 config 802.1x reauth

Purpose

To reauthenticate the device connected with the port.

Format

config 802.1x reauth [port_based ports [<portlist> | all] | mac_based ports [<portlist> | all] {mac_address <macaddr>}]

Description

This command is used to reauthenticate the device connected with the port. During the reauthentication period, the port status remains authorized until failed reauthentication.

Parameters

Parameters	Description
port_based	The switch passes data based on its authenticated port.
mac_based	The switch passes data based on the MAC address of authenticated RADIUS client.
portlist	Specify a range of ports to be configured.
all	All ports.
mac_address	The MAC address of the authenticated RADIUS client.

Restrictions

Only Administrator-level users can issue this command.

Examples

To reauthenticate the device connected with the port:

```
DGS-3200-10:4# config 802.1x reauth port_based ports all
Command: config 802.1x reauth port_based ports all

Success.

DGS-3200-10:4#
```

55-16 create 802.1x guest_vlan

Purpose

To assign a static VLAN to be a guest VLAN.

Format

create 802.1x guest_vlan {<vlan_name 32>}

Description

This command is used to assign a static VLAN to be a guest VLAN.

Parameter

Parameters	Description
vlan_name 32	Specify the static VLAN to be a guest VLAN.

Restrictions

Only Administrator-level users can issue this command. The specific VLAN which is assigned to a guest VLAN must already exist. The specific VLAN which is assigned to the guest VLAN can't be deleted.

Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3200-10:4# create 802.1x guest_vlan guestVLAN
Command: create 802.1x guest_vlan guestVLAN

Success.

DGS-3200-10:4#
```

55-17 delete 802.1x guest_vlan

Purpose

To delete a guest VLAN configuration.

Format

delete 802.1x guest_vlan {<vlan_name 32>}

Description

This command is used to delete a guest VLAN setting, but not to delete the static VLAN itself.

Parameter

Parameters	Description
vlan_name 32	The guest VLAN name.

Restrictions

Only Administrator-level users can issue this command. All ports which are enabled as guest VLAN will return to the original VLAN after the guest VLAN is deleted.

Example

To delete a guest VLAN configuration:

```
DGS-3200-10:4# delete 802.1x guest_vlan guestVLAN
Command: delete 802.1x guest_vlan guestVLAN

Success.

DGS-3200-10:4#
```

55-18 config 802.1x guest vlan

Purpose

To configure a guest VLAN setting.

Format

config 802.1x guest_vlan ports [<portlist>|all] state [enable | disable]

Description

This command is used to configure a guest VLAN setting.

Parameter

Parameters	Description
ports	A range of ports to enable or disable the guest VLAN function
all	All ports.
state	Specify the guest VLAN port state of the configured ports. **enable**: join to the guest VLAN. **disable**: remove from guest VLAN.

Restrictions

Only Administrator-level users can issue this command. If the specific port state is changed from the enabled state to the disabled state, this port will move to its original VLAN.

Example

To configure a guest VLAN setting for ports 1 to 8:

```
DGS-3200-10:4# config 802.1x guest_vlan ports 1-8 state enable
Command: config 802.1x guest_vlan ports 1-8 state enable

Warning! The ports are moved to Guest VLAN.

Success.

DGS-3200-10:4#
```

55-19 show 802.1x guest_vlan

Purpose

To display the guest VLAN setting.

Format

show 802.1x guest _vlan

Description

This command is used to display guest VLAN information.

Parameter

None.

Restrictions

None.

Example

To display guest VLAN information:

```
DGS-3200-10:4#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-------------------------------------------------------------
Guest VLAN : guest
Enable Guest VLAN Ports : 1-10

DGS-3200-10:4#
```

55-20 config radius add

Purpose

To add a new RADIUS server. The server with a lower index has a higher authentication priority.

Format

config radius add <server_index 1-3> [<server_ip> | <ipv6addr>] key <password 32> [default | {auth_port <udp_port_number 1-65535 > | acct_port <udp_port_number 1-65535 > | timeout <sec 1-255> | retransmit<int 1-20>}]

Description

This command is used to add a new RADIUS server.

Parameters

Parameters	Description
server_index	The RADIUS server index.
server_ip	The IP address of the RADIUS server.
ipv6addr	The IPv6 address of the RADIUS server.
key	The key pre-negotiated between switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.
default	Set the **auth_port** to be 1812 and **acct_port** to be 1813.
auth_port	Specify the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server. The range is 1 to 65535.
acct_port	Specify the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server. The range is 1 to 65535.
timeout	The time in second for waiting server reply. The default value is 5

	seconds.
retransmit	The count for re-transmit. The default value is 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a new RADIUS server:

```
DGS-3200-10:4#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DGS-3200-10:4#
```

55-21 config radius delete

Purpose

To delete a RADIUS server.

Format

config radius delete <server_index 1-3>

Description

This command is used to delete a RADIUS server.

Parameters

Parameters	Description
server_index	The RADIUS server index. The range is from 1 to 3.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a RADIUS server:

```
DGS-3200-10:4#config radius delete 1
Command: config radius delete 1

Success.

DGS-3200-10:4#
```

55-22 config radius

Purpose

To configure a RADIUS server.

Format

config radius <server_index 1-3> {ipaddress [<server_ip> | <ipv6addr>] | key <password 32> | auth_port [<udp_port_number 1-65535> | default] | acct_port [<udp_port_number 1-65535> | default] | timeout [<sec 1-255> | default] | retransmit [<int 1-20> | default]}

Description

This command is used to configure a RADIUS server.

Parameters

Parameters	Description
server_index	The RADIUS server index.
server_ip	The IP address of the RADIUS server.
ipv6addr	The IPv6 address.
key	The IPv6 address of the RADIUS server.
passwd	The key pre-negotiated between the switch and the RADIUS server. It is used to encrypt user's authentication data before being transmitted over the Internet. The maximum length of the key is 32.
auth_port	Specify the UDP port number which is used to transmit RADIUS authentication data between the switch and the RADIUS server. Specify **default** to have the value of 1813.
acct_port	Specify the UDP port number which is used to transmit RADIUS accounting statistics between the switch and the RADIUS server. Specify **default** to have the value of 5.
timeout	The time in second for waiting server reply. The default value is 5 seconds. Specify **default** to have the value of 5.
retransmit	The count for re-transmit. Specify **default** to have the value of 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a RADIUS server:

```
DGS-3200-10:4#config radius 1 ipaddress 10.48.74.121 key dlink timeout 10
Command: config radius 1 ipaddress 10.48.74.121 key dlink timeout 10


Success.
```

```
DGS-3200-10:4#
```

55-23 show radius

Purpose

To display RADIUS server configurations.

Format

show radius

Description

This command is used to display the RADIUS server configurations.

Parameters

None.

Restrictions

None.

Examples

To display RADIUS server configurations:

```
DGS-3200-10:4# show radius
Command: show radius

Index 1
   IP Address     : fe80:fec0:56ab:34b0:20b2:6aff:fecf:7ec6
   Auth-Port      : 1812
   Acct-Port      : 1813
   Timeout        : 5
   Retransmit     : 2
   Key            : adfdslkfjefiefdkgjdassdwtgjk6y1w

Index 2
   IP Address     : 172.18.211.71
   Auth-Port      : 1812
   Acct-Port      : 1813
   Timeout        : 5
   Retransmit     : 2
   Key            : 1234567
```

```
Index 3
   IP Address     : 172.18.211.108
   Auth－Port     : 1812
   Acct－Port     : 1813
   Timeout        : 5
   Retransmit     : 2
   Key            : adfdslkfjefiefdkgjdassdwtgjk6y1w



DGS-3200-10:4#
```

55-24 show auth_statistics

Purpose

To display authenticator statistics information

Format

show auth_statistics {ports <portlist>}

Description

This command is used to display authenticator statistics information

Parameters

Parameters	Description
ports	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display authenticator statistics information from port 1:

```
DGS-3200-10:4#show auth_statistics ports 1
Command: show auth_statistics ports 1

Port number : 1

EapolFramesRx                          0
EapolFramesTx                          6
EapolStartFramesRx                    0
EapolReqIdFramesTx                    6
EapolLogoffFramesRx                   0
EapolReqFramesTx                      0
EapolRespIdFramesRx                   0
EapolRespFramesRx                     0
InvalidEapolFramesRx                  0
EapLengthErrorFramesRx                0
LastEapolFrameVersion                 0
LastEapolFrameSource                  00-00-00-00-00-00

DGS-3200-10:4#
```

55-25 show auth_diagnostics

Purpose

To display authenticator diagnostics information

Format

show auth_diagnostics {ports <portlist>}

Description

This command is used to display authenticator diagnostics information.

Parameters

Parameters	Description
ports	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display authenticator diagnostics information from port 1:

```
DGS-3200-10:4# show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port number : 1

EntersConnecting                      20
EapLogoffsWhileConnecting             0
EntersAuthenticating                  0
SuccessWhileAuthenticating            0
TimeoutsWhileAuthenticating           0
FailWhileAuthenticating               0
ReauthsWhileAuthenticating            0
EapStartsWhileAuthenticating          0
EapLogoffWhileAuthenticating          0
ReauthsWhileAuthenticated             0
EapStartsWhileAuthenticated           0
EapLogoffWhileAuthenticated           0
BackendResponses                      0
BackendAccessChallenges               0
BackendOtherRequestsToSupplicant      0
BackendNonNakResponsesFromSupplicant  0
BackendAuthSuccesses                  0
BackendAuthFails                      0

DGS-3200-10:4#
```

55-26 show auth_session_statistics

Purpose

To display authenticator session statistics information.

Format

show auth_session_statistics {ports <portlist>}

Description

This command is used to display authenticator session statistics information.

Parameters

Parameters	Description
ports	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display authenticator session statistics information from port 1:

```
DGS-3200-10:4#show auth_statistics ports 1
Command: show auth_statistics ports 1



 MAC Address : 00-0C-6E-AA-B9-C0
 Port Number : 1

 EapolFramesRx                          0
 EapolFramesTx                          13
 EapolStartFramesRx                     0
 EapolReqIdFramesTx                     12
 EapolLogoffFramesRx                    0
 EapolReqFramesTx                       0
 EapolRespIdFramesRx                    0
 EapolRespFramesRx                      0
 InvalidEapolFramesRx                   0
 EapLengthErrorFramesRx                 0

 LastEapolFrameVersion                  0
 LastEapolFrameSource                   00-00-00-00-00-00



CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

55-27 show auth_client

Purpose

To display authentication client information.

Format

show auth_client

Description

This command is used to display authentication client information.

Parameters

None.

Restrictions

None

Examples

To display authentication client information:

```
DGS-3200-10:4#show auth_client
Command: show auth_client

 radiusAuthClient ==>
 radiusAuthClientInvalidServerAddresses   0
 radiusAuthClientIdentifier

 radiusAuthServerEntry ==>
 radiusAuthServerIndex :3

 radiusAuthServerAddress                  0.0.0.0
 radiusAuthClientServerPortNumber         0
 radiusAuthClientRoundTripTime            0
 radiusAuthClientAccessRequests           0
 radiusAuthClientAccessRetransmissions    0
 radiusAuthClientAccessAccepts            0
 radiusAuthClientAccessRejects            0
 radiusAuthClientAccessChallenges         0
 radiusAuthClientMalformedAccessResponses 0
 radiusAuthClientBadAuthenticators        0
 radiusAuthClientPendingRequests          0
 radiusAuthClientTimeouts                 0
 radiusAuthClientUnknownTypes             0
 radiusAuthClientPacketsDropped           0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

55-28 show acct_client

Purpose

To display account client information.

Format

show acct_client

Description

This command is used to display account client information

Parameters

None.

Restrictions

None.

Examples

To display account client information:

```
DGS-3200-10:4# show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier               D-Link



radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                   0.0.0.0
radiusAccClientServerPortNumber          X
radiusAccClientRoundTripTime             0
radiusAccClientRequests                  0
radiusAccClientRetransmissions           0
radiusAccClientResponses                 0
radiusAccClientMalformedResponses        0
radiusAccClientBadAuthenticators         0
radiusAccClientPendingRequests           0
radiusAccClientTimeouts                  0
radiusAccClientUnknownTypes              0
radiusAccClientPacketsDropped            0

CTRL+C ESC q Quit SPACE n Next Page p Previous Page r Refresh
```

55-29 config accounting service

Purpose

To configure the state of the specified RADIUS accounting service.

Format

config accounting service [network|shell|system] state [enable|disable]

Description

This command allows the user to enable or disable the specified RADIUS accounting service.

Parameters

Parameters	Description
network	Specify the accounting service for 802.1X port access control. By default, the service is disabled.
shell	Specify the accounting service for shell events. When a user logins or logouts of the switch (via the console, Telnet, or SSH) and when timeout occurs, accounting information will be collected and sent to the RADIUS server. By default, the service is disabled.
system	Specify the accounting service for system events: reset and reboot. By default, the service is disabled.
state	Specify to enable or disable the accounting service.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the state of the RADIUS accounting service shell to enable:

```
DGS-3200-10:4#config accounting service shell state enable
Command: config accounting service shell state enable

Success

DGS-3200-10:4#
```

55-30 show accounting service

Purpose

To display RADIUS accounting service information.

Format

show accounting service

Description

This command is used to display RADIUS accounting service information.

Parameters

None.

Restrictions

None.

Examples

To display accounting service information:

```
DGS-3200-10:4# show accounting service
Command: show accounting service

Accounting State
-------------------
Network : Disabled
Shell   : Disabled
System  : Disabled

DGS-3200-10:4#
```

56 Access Authentication Control Command List

enable authen_policy
disable authen_policy
show authen_policy
create authen_login method_list_name <string 15>
config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}
delete authen_login method_list_name <string 15>
show authen_login [default | method_list_name <string 15> | all]
create authen_enable method_list_name <string 15>
config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}
delete authen_enable method_list_name <string 15>
show authen_enable [default | method_list_name <string 15> | all]
config authen application [console | telnet | ssh | http |all] [login | enable] [default| method_list_name <string 15>]
show authen application
create authen server_group <string 15>
config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group <string 15>
show authen server_group {<string 15>}
create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}
delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host
config authen parameter response_timeout <int 0-255>
config authen parameter attempt <int 1-255>
show authen parameter
enable admin
config admin local_enable {encrypt [plain_text | sha_1] <password>}

56-1 enable authen_policy

Purpose

To enable system access authentication policy.

Format

enable authen_policy

Description

This command is used to enable system access authentication policy. When enabled, the device will adopt the login authentication method list to authenticate the user for login, and adopt the enable authentication method list to authenticate the enable password for promoting the user‘s privilege to Administrator level.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable system access authentication policy:

```
DGS-3200-10:4#enable authen_policy
Command: enable authen_policy

Success.

DGS-3200-10:4#
```

56-2 disable authen_policy

Purpose

To disable system access authentication policy.

Format

disable authen_policy

Description

This command is used to disable system access authentication policy. When authentication is disabled, the device will adopt the local user account database to authenticate the user for login, and adopt the local enable password to authenticate the enable password for promoting the user‘s privilege to Administrator level.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable system access authentication policy:

```
DGS-3200-10:4#disable authen_policy
Command: disable authen_policy

Success.

DGS-3200-10:4#
```

56-3 show authen_policy

Purpose

To display whether system access authentication policy is enabled or disabled.

Format

show authen_policy

Description

This command is used to display whether system access authentication policy is enabled or disabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display system access authentication policy:

```
DGS-3200-10:4#show authen_policy
Command: show authen_policy

Authentication Policy : Enabled

DGS-3200-10:4#
```

56-4 create authen_login method_list_name

Purpose

To create a user-defined method list of authentication methods for user login.

Format

create authen_login method_list_name <string 15>

Description

This command is used to create a user-defined method list of authentication methods for user login. The maximum supported number of the login method lists is eight.

Parameters

Parameters	Description
<string 15>	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a user-defined method list for user login:

```
DGS-3200-10:4#create authen_login method_list_name login_list_1
Command: create authen_login method_list_name login_list_1

Success.

DGS-3200-10:4#
```

56-5 config authen_login

Purpose

To configure a user-defined or default method list of authentication methods for user login.

Format

config authen_login [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}

Description

This command is used to configure a user-defined or default method list of authentication methods for user login. The sequence of methods will affect the authentication result. For example, if the sequence is TACACS+ first, then TACACS and local, when a user tries to login, the authentication request will be sent to the first server host in the TACACS+ built-in server group. If the first server host in the TACACS+ group

is missing, the authentication request will be sent to the second server host in the TACACS+ group, and so on. If all server hosts in the TACACS+ group are missing, the authentication request will be sent to the first server host in the TACACS group. If all server hosts in a TACACS group are missing, the local account database in the device is used to authenticate this user. When a user logs in to the device successfully while using methods like TACACS/XTACACS/TACACS+/RADIUS built-in or user-defined server groups or none, the “user” privilege level is assigned only. If a user wants to get admin privilege level, the user must use the “enable admin” command to promote his privilege level. But when the local method is used, the privilege level will depend on this account privilege level stored in the local device.

Parameters

Parameters	Description
default	The default method list of authentication methods.
method_list_name <string 15>	The user-defined method list of authentication methods.
tacacs	Authentication by the built-in server group **tacacs**.
xtacacs	Authentication by the built-in server group **xtacacs**.
tacacs+	Authentication by the built-in server group **tacacs+**.
radius	Authentication by the built-in server group **radius**.
server_group <string 15>	Authentication by the user-defined server group.
local	Authentication by local user account database in device.
none	No authentication.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a user-defined method list for user login:

```
DGS-3200-10:4#config authen_login method_list_name login_list_1 method tacacs+
tacacs local
Command: config authen_login method_list_name login_list_1 method tacacs+ tacac
s local

Success.

DGS-3200-10:4#
```

56-6 delete authen_login method_list_name

Purpose

To delete a user-defined method list of authentication methods for user login.

Format

delete authen_login method_list_name <string 15>

Description

This command is used to delete a user-defined method list of authentication methods for user login.

Parameters

Parameters	Description
<string 15>	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a user-defined method list for user login:

```
DGS-3200-10:4#delete authen_login method_list_name login_list_1
Command: delete authen_login method_list_name login_list_1

Success.

DGS-3200-10:4#
```

56-7 show authen_login

Purpose

To display the method list of authentication methods for user login.

Format

show authen_login [default | method_list_name <string 15> | all]

Description

This command is used to display the method list of authentication methods for user login.

Parameters

Parameters	Description
default	Display default user-defined method list for user login.
method_list_name	Display the specific user-defined method list for user login.

all	Display all method lists for user login.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display a user-defined method list for user login:

```
DGS-3200-10:4#show authen_login method_list_name login_list_1
Command: show authen_login method_list_name login_list_1

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
login_list_1      1         tacacs+          Built-in Group
                  2         tacacs           Built-in Group
                  3         mix_1            User-defined Group
                  4         local            Keyword

DGS-3200-10:4#
```

56-8 create authen_enable method_list_name

Purpose

To create a user-defined method list of authentication methods for promoting a user's privilege to Administrator level.

Format

create authen_enable method_list_name <string 15>

Description

This command is used to create a user-defined method list of authentication methods for promoting a user's privilege to Admin level. The maximum supported number of the enable method lists is eight.

Parameters

Parameters	Description
<string 15>	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a user-defined method list for promoting a user's privilege to Admin level:

```
DGS-3200-10:4#create authen_enable method_list_name enable_list_1
Command: create authen_enable method_list_name enable_list_1

Success.

DGS-3200-10:4#
```

56-9 config authen_enable

Purpose

To configure a user-defined or default method list of authentication methods for promoting a user's privilege to Administrator level.

Format

config authen_enable [default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local _enable | none}

Description

This command is used to configure a user-defined or default method list of authentication methods for promoting a user's privilege to Admin level. The sequence of methods will affect the authentication result. For example, if the sequence is TACACS+ first, then TACACS and local_enable, when a user tries to login, the authentication request will be sent to the first server host in the TACACS+ built-in server group. If the first server host in the TACACS+ group is missing, the authentication request will be sent to the second server host in the TACACS+ group, and so on. If all server hosts in the TACACS+ group are missing, the authentication request will be sent to the first server host in the TACACS group. If all server hosts in the TACACS group are missing, the local enable password in the device is used to authenticate this user's password. The local enable password in the device can be configured by the CLI command "config admin local_password".

Parameters

Parameters	Description
default	The default method list of authentication methods.
method_list_name <string 15>	The user-defined method list of authentication methods.
tacacs	Authentication by the built-in server group **tacacs**.
xtacacs	Authentication by the built-in server group **xtacacs**.
tacacs+	Authentication by the built-in server group **tacacs+**.
radius	Authentication by the built-in server group **radius**.

server_group <string 15>	Authentication by the user-defined server group.
local_enable	Authentication by local enable password in device.
none	No authentication.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a user-defined method list for promoting a user's privilege to Admin level:

```
DGS-3200-10:4#config authen_enable method_list_name enable_list_1 method tacacs+
tacacs local_enable
Command: config authen_ enable method_list_name enable_list_1 method tacacs+ tacac
s local_enable

Success.

DGS-3200-10:4#
```

56-10 delete authen_enable method_list_name

Purpose

To delete a user-defined method list of authentication methods for promoting a user's privilege to Administrator level.

Format

delete authen_enable method_list_name <string 15>

Description

This command is used to delete a user-defined method list of authentication methods for promoting a user's privilege to Administrator level.

Parameters

Parameters	Description
<string 15>	The user-defined method list name

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a user-defined method list for promoting a user's privilege to Admin level:

```
DGS-3200-10:4#delete authen_enable method_list_name enable_list_1
Command: delete authen_enable method_list_name enable_list_1

Success.

DGS-3200-10:4#
```

56-11 show authen_enable

Purpose

To display the method list of authentication methods for promoting a user's privilege to Administrator level.

Format

show authen_enable [default | method_list_name <string 15> | all]

Description

This command is used to display the method list of authentication methods for promoting a user's privilege to Administrator level.

Parameters

Parameters	Description
default	Display the default user-defined method list for promoting a user's privilege to Administrator level.
method_list_name <string 15>	Display the specific user-defined method list for a promoting user's privilege to Administrator level.
all	Display all method lists for promoting a user's privilege to Administrator level.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display all method lists for promoting a user's privilege to Administrator level:

```
DGS-3200-10:4#show authen_enable all
Command: show authen_enable all

Method List Name  Priority  Method Name      Comment
----------------  --------  ---------------  ------------------
default           1          local_enable     Keyword

Total Entries : 1

DGS-3200-10:4#
```

56-12 config authen application

Purpose

To configure login or enable method list for all or the specified application.

Format

config authen application [console | telnet | ssh | http |all] [login | enable] [default| method_list_name <string 15>]

Description

This command is used to configure login or enable method list for all or the specified application.

Parameters

Parameters	Description
console	Specify the application as console.
telnet	Specify the application as Telnet.
ssh	Specify the application as SSH.
http	Specify the application as web.
all	Specify all applications including **console**, **telnet**, **ssh**, and **web**.
login	Select the method list of authentication methods for user login.
enable	Select the method list of authentication methods for promoting user's privilege to Admin level.
default	The default method list.
method_list_name	The user-defined method list name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the login method list for Telnet:

```
DGS-3200-10:4#config authen application telnet login method_list_name
login_list_1
Command: config authen application telnet login method_list_name login_list_1

Success.

DGS-3200-10:4#
```

56-13 show authen application

Purpose

To display the login/enable method list for all applications.

Format

show authen application

Description

This command is used to display the login/enable method list for all applications.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the login/enable method list for all applications:

```
DGS-3200-10:4#show authen application
Command: show authen application

Application  Login Method List  Enable Method List
-----------  -----------------  ------------------
Console      default            default
Telnet       login_list_1       default
SSH          default            default
HTTP         default            default

DGS-3200-10:4#
```

56-14 create authen server_group

Purpose

To create a user-defined authentication server group.

Format

create authen server_group <string 15>

Description

This command is used to create a user-defined authentication server group. The maximum supported number of server groups including built-in server groups is eight. Each group consists of eight server hosts as maximum.

Parameters

Parameters	Description
<string 15>	The user-defined server group name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a user-defined authentication server group:

```
DGS-3200-10:4#create authen server_group mix_1
Command: create authen server_group mix_1

Success.

DGS-3200-10:4#
```

56-15 config authen server_group

Purpose

To add or remove an authentication server host to or from the specified server group.

Format

config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

Description

This command is used to add or remove an authentication server host to or from the specified server group. Built-in server group **tacacs**, **xtacacs**, **tacacs+**, and **radius** accept the server host with the same protocol only, but user-defined server group can accept server hosts with different protocols. The server host must be created first by using the CLI command **create authen server_host**.

Parameters

Parameters	Description
server_group tacacs	The built-in server group **tacacs**.
server_group xtacacs	The built-in server group **xtacacs**.
server_group tacacs+	The built-in server group **tacacs+**.
server_group radius	The built-in server group **radius**.
server_group <string 15>	A user-defined server group.
add	Add a server host to a server group.
delete	Remove a server host from a server group.
server_host <ipaddr>	The server host's IP address.
protocol tacacs	The server host's authentication protocol.
protocol xtacacs	The server host's authentication protocol.
protocol tacacs+	The server host's authentication protocol.
protocol radius	The server host's authentication protocol.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add an authentication server host to a server group:

```
DGS-3200-10:4#config authen server_group mix_1 add server_host 10.1.1.222 protoc
ol tacacs+
Command: config authen server_group mix_1 add server_host 10.1.1.222 protocol ta
cacs+

Success.

DGS-3200-10:4#
```

56-16 delete authen server_group

Purpose

To delete a user-defined authentication server group.

Format

delete authen server_group <string 15>

Description

This command is used to delete a user-defined authentication server group.

Parameters

Parameters	Description
<string 15>	The user-defined server group name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a user-defined authentication server group:

```
DGS-3200-10:4#delete authen server_group mix_1
Command: delete authen server_group mix_1

Success.

DGS-3200-10:4#
```

56-17 show authen server_group

Purpose

To display the authentication server groups.

Format

show authen server_group {<string 15>}

Description

This command is used to display the authentication server groups.

Parameters

Parameters	Description
<string 15>	The built-in or user-defined server group name.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display all authentication server groups:

```
DGS-3200-10:4#show authen server_group
Command: show authen server_group

Group Name        IP Address        Protocol
---------------  ---------------  --------
mix_1             10.1.1.222        TACACS+

radius            --------------------------

tacacs            --------------------------

tacacs+           10.1.1.222        TACACS+

xtacacs           --------------------------

Total Entries : 5

DGS-3200-10:4#
```

56-18 create authen server_host

Purpose

To create an authentication server host.

Format

create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int

1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Description

This command is used to create an authentication server host. When an authentication server host is created, the IP address and protocol are the index. That means more than one authentication protocol service can be run on the same physical host. The maximum supported number of server hosts is 16.

Parameters

Parameters	Description	
<ipaddr>	The server host's IP address.	
protocol tacacs	The server host's authentication protocol.	
protocol xtacacs	The server host's authentication protocol.	
protocol tacacs+	The server host's authentication protocol.	
protocol radius	The server host's authentication protocol.	
port	The port number of the authentication protocol for the server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812.	
key	**<key_string 254>**	The key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.
	none	No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.
timeout	The time in seconds for waiting for a server reply. Default value is 5 seconds.	
retransmit	The count for re-transmit. This value is meaningless for TACACS+. Default value is 2.	

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a TACACS+ authentication server host with a listening port number of 15555 and a timeout value of 10 seconds:

```
GS-3200-10:4#create authen server_host 10.1.1.222 protocol tacacs+ port 15555 t
imeout 10
Command: create authen server_host 10.1.1.222 protocol tacacs+ port 15555 timeou
t 10

Key is empty for TACACS+ or RADIUS.
Success.

DGS-3200-10:4#
```

56-19 config authen server_host

Purpose

To configure an authentication server host.

Format

cconfig authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-20>}

Description

This command is used to configure an authentication server host.

Parameters

Parameters	Description	
<ipaddr>	The server host's IP address.	
protocol tacacs	The server host's authentication protocol.	
protocol xtacacs	The server host's authentication protocol.	
protocol tacacs+	The server host's authentication protocol.	
protocol radius	The server host's authentication protocol.	
port	The port number of the authentication protocol for the server host. The default value for TACACS/XTACACS/TACACS+ is 49. The default value for RADIUS is 1812.	
key	**<key_string 254>**	The key for TACACS+ and RADIUS authentication. If the value is null, no encryption will apply. This value is meaningless for TACACS and XTACACS.
	none	No encryption for TACACS+ and RADIUS authentication. This value is meaningless for TACACS and XTACACS.
timeout	The time in seconds for waiting for a server reply. The default value is 5 seconds.	
retransmit	The count for re-transmit. This value is meaningless for TACACS+.	

	The default value is 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a TACACS+ authentication server host's key value:

```
DGS-3200-10:4#config authen server_host 10.1.1.222 protocol tacacs+ key "This is
 a secret."
Command: config authen server_host 10.1.1.222 protocol tacacs+ key "This is a se
cret."

Success.

DGS-3200-10:4#
```

56-20 delete authen server_host

Purpose

To delete an authentication server host.

Format

delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]

Description

This command is used to delete an authentication server host.

Parameters

Parameters	Description
server_host <ipaddr>	The server host's IP address.
protocol tacacs	The server host's authentication protocol.
protocol xtacacs	The server host's authentication protocol.
protocol tacacs+	The server host's authentication protocol.
protocol radius	The server host's authentication protocol.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an authentication server host:

```
DGS-3200-10:4#delete authen server_host 10.1.1.222 protocol tacacs+
Command: delete authen server_host 10.1.1.222 protocol tacacs+

Success.

DGS-3200-10:4#
```

56-21 show authen server_host

Purpose

To display the authentication server hosts.

Format

show authen server_host

Description

This command is used to display authentication server hosts.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display all authentication server hosts:

```
DGS-3200-10:4#show authen server_host
Command: show authen server_host

IP Address       Protocol  Port   Timeout  Retransmit  Key
---------------  --------  -----  -------  ----------  -------------------------
10.1.1.222       TACACS+   15555  10       ------      This is a secret.

Total Entries : 1

DGS-3200-10:4#
```

56-22 config authen parameter response_timeout

Purpose

To configure the amount of time waiting or for user input on console, Telnet, and SSH applications.

Format

config authen parameter response_timeout <int 0-255>

Description

This command is used to configure the amount of time waiting or for user input on console, Telnet, and SSH applications.

Parameters

Parameters	Description
<int 0-255>	The amount of time for user input on console or Telnet or SSH. 0 means there is no time out. The default value is 30 seconds.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the amount of time waiting or for user input to be 60 seconds:

```
DGS-3200-10:4#config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3200-10:4#
```

56-23 config authen parameter attempt

Purpose

To configure the maximum attempts for users trying to login or promote the privilege on console or Telnet, applications.

Format

config authen parameter attempt <int 1-255>

Description

This command is used to configure the maximum attempts for users trying to login or promote the privilege on console or Telnet applications. If the failure value is exceeded, connection or access will be locked.

Parameters

Parameters	Description
<int 1-255>	The amount of attempts for users trying to login or promote the privilege on console or Telnet. The default value is 3.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the maximum attempts for users trying to login or promote the privilege to be 9:

```
DGS-3200-10:4#config authen parameter attempt 9
Command: config authen parameter attempt 9

Success.

DGS-3200-10:4#
```

56-24 show authen parameter

Purpose

To display the parameters of authentication.

Format

show authen parameter

Description

This command is used to display the authentication parameters.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the authentication parameters:

```
DGS-3200-10:4#show authen parameter
Command: show authen parameter

Response Timeout : 60 seconds
User Attempts    : 9

DGS-3200-10:4#
```

56-25 enable admin

Purpose

To open the administrator level privilege

Format

enable admin

Description

This command is used to promote the "user" privilege level to "admin" level. When the user enters this command, the authentication method TACACS, XTACAS, TACACS+, user-defined server groups, local enable, or none will be used to authenticate the user. Because TACACS, XTACACS and RADIUS don't support the **enable** function by themselves, if a user wants to use either one of these three protocols to enable authentication, the user must create a special account on the server host first, which has a username **enable** and then configure its password as the enable password to support the "enable" function. This command can not be used when authentication policy is disabled.

Parameters

None.

Restrictions

None.

Examples

To enable administrator lever privilege:

```
DGS-3200-10:3#enable admin
Password:********

DGS-3200-10:4#
```

56-26 config admin local_enable

Purpose

To configure the local enable password for the administrator level privilege.

Format

config admin local_enable <password 0-15>

config admin local_enable {encrypt [plain_text | sha_1] <password>}

Description

This command is used to configure the local enable password for the enable command. When the user chooses the **local_enable** method to promote the privilege level, the enable password of the local device is needed.

Parameters

Parameters	Description
plain_text	Specify the password in plain text form.
sha_1	Specify the password in SHA-1 encrypted form.
<password>	The specific password.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the administrator password:

```
DGS-3200-10:4#config admin local_enable
Command: config admin local_enable

Enter the old password:
Enter the case-sensitive new password:******
Enter the new password again for confirmation:******
Success.

DGS-3200-10:4#
```

57 SSL Command List

download ssl certificate <ipaddr> certfilename <path_filename 64> {keyfilename <path_filename 64>}
config ssl certificate chain [default | <cert_list>]
delete ssl certificate <path_filename 64>
enable ssl { ciphersuite { RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 } }
disable ssl { ciphersuite { RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 } }
show ssl {certificate {<path_filename 64>}}
show ssl certificate chain
show ssl cachetimout
config ssl cachetimout <value 60-86400>

57-1 download ssl certificate

Purpose

To download certificate to device according to certificate level.

Format

download ssl certificate <ipaddr> certfilename <path_filename 64> {keyfilename <path_filename 64>}

Description

This command is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication.

Parameters

Parameters	Description
<ipaddr>	Input the TFTP server IP address.
certfilename	Specify the certificate file path in respect to the TFTP server root path..
keyfilename	Specify the private key file path which accompanies the certificate.

Restrictions

Only Administrator-level users can issue this command.

Examples

To download a certificate from a TFTP server:

```
DGS-3200-10:4# download ssl certificate 10.55.47.1 certfilename cert.cer
keyfilename private.key
Command: download ssl certificate 10.55.47.1 certfilename cert.cer keyfilename
private.key

Certificate Loaded Successfully.

DGS-3200-10:4#
```

57-2 config ssl certificate chain

Purpose

To specify chain of certifications on the Switch.

Format

config ssl certificate chain [default | <cert_list>]

Description

This command is used to specify chain of certifications on the Switch. The format of the certificate should be kept consistent.

Parameters

Parameters	Description
default	Enter this parameter to use the build-in certification on the Switch.
<cert_list>	Specify chain of certifications on the Switch.

Restrictions

Only Administrator-level users can issue this command.

Examples

To config ssl cachain:

```
DGS-3200-10:4#config ssl certificate chain tongken.cer,web_ca2.cer,server.crt
Command: config ssl certificate chain tongken.cer,web_ca2.cer,server.crt

Success.

DGS-3200-10:4#
```

57-3 delete ssl certificate

Purpose

To delete a certificate on the Switch.

Format

delete ssl certificate <path_filename 64>

Description

This command is used to delete a certificate on the Switch.

Parameters

Parameters	Description
<path_filename 64>	Specify certification name on the Switch.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a certificate.

```
DGS-3200-10:4# delete ssl certificate web_ca2.cer
Command: delete ssl certificate web_ca2.cer

Success.

DGS-3200-10:4#
```

57-4 enable ssl

Purpose

To enable the SSL feature and ciphersuites.

Format

enable ssl { ciphersuite { RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 } }

Description

This command is used to enable the SSL status and its individual ciphersuites. Using the **enable ssl** command will enable the SSL feature, which means SSLv3 and TLSv1. Each ciphersuite must be enabled by this command.

Parameters

Parameters	Description
ciphersuite	For configuring a cipher suite combination.
RSA_with_RC4_128_MD5	Indicate RSA key exchange with RC4 128 bits encryption and MD5 hash.
RSA_with_3DES_EDE_CBC_SHA	Indicate RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
DHE_DSS_with_3DES_EDE_CBC_SHA	Indicate DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
RSA_EXPORT_with_RC4_40_MD5	Indicate RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.
NULL	Enable the SSL feature.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3200-10:4# enable ssl ciphersuite RSA_with_RC4_128_MD5
Command: enable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3200-10:4#
```

To enable SSL:

```
DGS-3200-10:4# enable ssl
Command: enable ssl

Note: Web will be disabled if SSL is enabled.
Success.

DGS-3200-10:4#
```

57-5 disable ssl

Purpose

To disable SSL feature and ciphersuites.

Format

disable ssl { ciphersuite { RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5 } }

Description

This command is used to disable the SSL feature and supported ciphersuites.

Parameters

Parameters	Description
ciphersuite	For configuring cipher suite combination.
RSA_with_RC4_128_MD5	Indicate RSA key exchange with RC4 128 bits encryption and MD5 hash.
RSA_with_3DES_EDE_CBC_SHA	Indicate RSA key exchange with 3DES_EDE_CBC encryption and SHA hash.
DHE_DSS_with_3DES_EDE_CBC_SHA	Indicate DH key exchange with 3DES_EDE_CBC encryption and SHA hash.
RSA_EXPORT_with_RC4_40_MD5	Indicate RSA_EXPORT key exchange with RC4 40 bits encryption and MD5 hash.
NULL	Disable the SSL feature.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the SSL ciphersuite for RSA_with_RC4_128_MD5:

```
DGS-3200-10:4# disable ssl ciphersuite RSA_with_RC4_128_MD5
Command: disable ssl ciphersuite RSA_with_RC4_128_MD5

Success.

DGS-3200-10:4#
```

To disable the SSL feature:

```
DGS-3200-10:4# disable ssl
Command: disable ssl

Success.

DGS-3200-10:4#
```

57-6 show ssl

Purpose

To view the SSL status and the certificate file status on the Switch.

Format

show ssl {certificate {<path_filename 64>}}

Description

This command is used to view the SSL state and the certificate file status on the Switch.

Parameters

Parameters	Description
certificate	View the SSL certificate file information currently implemented on the Switch.
<path_filename 64>	Specify the certificate file path.

Restrictions

None.

Examples

To display the SSL status:

```
DGS-3200-10:4# show ssl
Commands: show ssl

SSL Status                                  Disabled
RSA_WITH_RC4_128_MD5                0x0004  Enabled
RSA_WITH_3DES_EDE_CBC_SHA           0x000A  Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA       0x0013  Enabled
RSA_EXPORT_WITH_RC4_40_MD5          0x0003  Enabled

DGS-3200-10:4#
```

To display all certificate:

```
DGS-3200-10:4# show ssl certificate
Command: show ssl certificate
   tongken.cer
   web_server.cer
   server.crt

DGS-3200-10:4#
```

To display the certificate file content:

```
DGS-3200-10:4# show ssl certificate server.crt
Command: show ssl certificate server.crt

Certificate Information:
Certificate Version :3
Serial Number :61:1E:65:CC:00:00:00:00:00:0B
Issuer Name   :CN=tongken
Subject Name  :CN=CA2
Not Before     :2010-09-10 06:40:50
Not After      :2011-09-10 06:50:50
Public Key Alg:rsaEncryption
Signed Using  :RSA+SHA1
RSA Key Size  :1024 bits

DGS-3200-10:4#
```

57-7 show ssl certificate chain

Purpose

To display chain of certifications on the Switch.

Format

show ssl certificate chain

Description

This command is used to display chain of certifications on the Switch.

Parameters

None.

Restrictions

None.

Examples

To show the SSL certificate chain:

```
DGS-3200-10:4#show ssl certificate chain
Command: show ssl certificate chain

tongken.cer,web_ca2.cer,server.crt

DGS-3200-10:4#
```

57-8 show ssl cachetimeout

Purpose

To display the SSL cache timeout value.

Format

show ssl cachetimeout

Description

This command is used to display the cache timeout value which is designed for a dlktimer library to remove the session ID after it has expired. In order to support the resume session feature, the SSL library keeps the session ID on the web server and invokes the dlktimer library to remove this session ID by the cache timeout value.

Parameters

None.

Restrictions

None.

Examples

To show the SSL cache timeout:

```
DGS-3200-10:4# show ssl cachetimeout
Commands: show ssl cachetimeout

Cache timeout is 600 second(s)

DGS-3200-10:4#
```

57-9 config ssl cachetimeout

Purpose

To configure the SSL cache timeout value. This value is between 1 minute and 24 hours.

Format

config ssl cachetimout <value 60-86400>

Description

This command is used to configure the cache timeout value which is designed for the dlktimer library to remove the session ID after expiration. In order to support the resume session feature, the SSL library keeps the session ID on the web server, and invokes the dlktimer library to remove this session ID by the cache timeout value. The unit of argument's value is second and its boundary is between 60 (1 minute) and 86400 (24 hours). The default value is 600 seconds.

Parameters

Parameters	Description
cachetimout	The SSL cache timeout value attributes.

Restrictions

None.

Examples

To configure an SSL cache timeout value of 60:

```
DGS-3200-10:4# config ssl cachetimeout 60
Commands: config ssl cachetimeout 60

Success.

DGS-3200-10:4#
```

58 SSH Command List

config ssh algorithm [3DES| AES128| AES192| AES256| arcfour|blowfish| cast128| twofish128| twofish192| twofish256| MD5| SHA1| RSA| DSA] [enable| disable]
show ssh algorithm
config ssh authmode [password|publickey|hostbased] [enable|disable]
show ssh authmode
config ssh user <username 15> authmode [publickey | password | hostbased [hostname <domain_name 32> |hostname_IP <domain_name 32> <ipaddr>]]
show ssh user authmode
config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail<int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}
enable ssh
disable ssh
show ssh server

58-1 config ssh algorithm

Purpose

To configure the SSH server algorithm.

Format

config ssh algorithm [3DES|AES128|AES192|AES256|arcfour|blowfish|cast128|twofish128| twofish192|twofish256|MD5|SHA1|RSA|DSS] [enable|disable]

Description

This command is used to configure the SSH service algorithm.

Parameters

Parameters	Description
3DES	An SSH server encryption algorithm.
blowfish	An SSH server encryption algorithm.
AES(128,192,256)	An SSH server encryption algorithm.
arcfour	An SSH server encryption algorithm.
cast128	An SSH server encryption algorithm.
twofish(128,192,256)	An SSH server encryption algorithm.
MD5	An SSH server data integrality algorithm.
SHA1	An SSH server data integrality algorithm.

DSS	An SSH server public key algorithm.
RSA	An SSH server public key algorithm.
enable	Used to enable the algorithm.
disable	Used to disable the alogirthm.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable an SSH server public key algorithm:

```
DGS-3200-10:4#config ssh algorithm DSA enable RSA enable
Command: config ssh algorithm DSA enable RSA enable

Success.

DGS-3200-10:4#
```

58-2 show ssh algorithm

Purpose

To show the SSH server algorithms.

Format

show ssh algorithm

Description

This command is used to display the SSH service algorithms.

Parameters

None.

Restrictions

None

Examples

To show the SSH server algorithms:

```
DGS-3200-10:4#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES        : Enabled
AES128      : Enabled
AES192      : Enabled
AES256      : Enabled
arcfour     : Enabled
blowfish    : Enabled
cast128     : Enabled
twofish128 : Enabled
twofish192 : Enabled
twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5         : Enabled
SHA1        : Enabled

Public Key Algorithm
--------------------------
RSA         : Enabled
DSA         : Enabled

DGS-3200-10:4#
```

58-3 config ssh authmode

Purpose

To update user authentication for SSH configuration.

Format

config ssh authmode [password|publickey|hostbased][enable|disable]

Description

This command is used to update the SSH user information.

Parameters

Parameters	Description
password	Specify user authentication method.
publickey	Specify user authentication method.
hostbased	Specify user authentication method.
enable	Enable user authentication method.
disable	Disable user authentication method.

Restrictions

Only Administrator-level users can issue this command.

Examples

To config the SSH user authentication method:

```
DGS-3200-10:4#config ssh authmode publickey enable
Command: config ssh authmode publickey enable

Success.

DGS-3200-10:4#
```

58-4 show ssh authmode

Purpose

To display user authentication method

Format

show ssh authmode

Description

This command is used to display the user authentication method.

Parameters

None.

Restrictions

None.

Examples

To display the SSH user authentication method:

```
DGS-3200-10:4#show ssh authmode
Command: show ssh authmode

The SSH Authentication Method:
Password    : Enabled
Public Key  : Enabled
Host-based  : Enabled



DGS-3200-10:4#
```

58-5 config ssh user

Purpose

To update user information for SSH configuration.

Format

config ssh user <username 15> authmode [publickey | password | hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>]]

Description

This command is used to update SSH user information

Parameters

Parameters	Description
username 15	The user name.
publickey	Specify user authentication method.
password	Specify user authentication method.
hostbased	Specify user authentication method.
hostname	Specify host domain name.
hostname_IP	Specify host domain name and IP address.
domain_name	Specify host name if configuration is in host-based mode.
ipaddr	Specify host IP address if configuring host-based mode.

Restrictions

Only Administrator-level users can issue this command.

Note: The user account must be created.

Examples

To update user “danilo” authmode:

```
DGS-3200-10:4#config ssh user danilo authmode publickey
Command: config ssh user danilo authmode publickey

Success.

DGS-3200-10:4#
```

58-6 show ssh user authmode

Purpose

To show SSH user information.

Format

show ssh user authmode

Description

This command is used to display SSH user information.

Parameters

None.

Restrictions

None.

Examples

To show user information about SSH configuration:

```
DGS-3200-10:4#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
User Name        Authentication Host Name                          Host IP
---------------- ---------      ---------------------------------- ---------------
admin            Password
danilo           Public Key
user             Password

Total Entries : 3



DGS-3200-10:4#
```

58-7 config ssh server

Purpose

To configure the SSH server.

Format

config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never] | port <tcp_port_number 1-65535>}

Description

This command is used to configure SSH server general information.

Parameters

Parameters	Description
maxsession	Specify SSH server max session at the same time.
contimeout	Specify SSH server connection timeout.
authfail	Specify user max fail attempts.
rekey	Specify time to re-generate session key.
never	Do not re-generate session key.
port	Specify the TCP port.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an SSH server max session of 3:

```
DGS-3200-10:4#config ssh server maxsession 3
Command: config ssh server maxsession 3


Success.


DGS-3200-10:4#
```

58-8 enable ssh

Purpose

To enable the SSH server.

Format

enable ssh server

Description

This command is used to enable SSH server services.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command. When enabling SSH, Telnet is disabled.

Examples

To enable SSH:

```
DGS-3200-10:4#enable ssh
Command: enable ssh


Success.


DGS-3200-10:4#
```

58-9 disable ssh

Purpose

To disable SSH server service.

Format

disable ssh server

Description

This command is used to disable SSH server services.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable SSH:

```
DGS-3200-10:4#disable ssh
Command: disable ssh

Success.

DGS-3200-10:4#
```

58-10 show ssh server

Purpose

To show SSH server information.

Format

show ssh server

Description

This command is used to display SSH server general information.

Parameters

None.

Restrictions

None.

Examples

To show SSH server:

```
DGS-3200-10:4#show ssh server
Command: show ssh server

The SSH Server Configuration
Maximum Session              : 8
Connection Timeout           : 120
Authentication Fail Attempts : 2
Rekey Timeout                : Never
TCP Port Number              : 22



DGS-3200-10:4#
```

59 IP-MAC-Port Binding (IMPB) Command List

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
create address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ports [<portlist> | all] {state [enable {[strict | loose] | [ipv6 | all]} | disable {[ipv6 | all]}] | mode [arp | acl] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500> }
config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}
config address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}
delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>| ipv6address <ipv6addr> mac_address <macaddr>]
show address_binding {ports {<portlist>}}
show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]
show address_binding ip_mac [all| [[ipaddress <ipaddr> | ipv6address <ipv6addr>] {mac_address <macaddr>} | mac_address <macaddr>]]
enable address_binding trap_log
disable address_binding trap_log
enable address_binding dhcp_snoop {[ipv6 | all]}
disable address_binding dhcp_snoop {[ipv6 | all]}
enable address_binding nd_snoop
disable address_binding nd_snoop
config address_binding nd_snoop ports [< portlist > | all] max_entry [< value 1-10 > | no_limit]
show address_binding nd_snoop {ports <portlist>}
show address_binding nd_snoop binding_entry {port <port>}
clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {[ipv6 | all]}
clear address_binding nd_snoop binding_entry ports [<portlist> | all]
show address_binding dhcp_snoop {max_entry {ports <portlist>}}
show address_binding dhcp_snoop binding_entry {port <port>}
config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}
config address_binding recover_learning ports

59-1 create address_binding ip_mac ipaddress

Purpose

To create an IP-MAC binding entry.

Format

create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Description

This command is used to create an IP-MAC binding entry.

Parameters

Parameters	Description
<ipaddr>	The IP address used to create this IP-MAC binding entry.
mac_address	The MAC address used to create this IP-MAC binding entry.
ports	Specify the portlist. If no ports are specified, the settings for this command will apply to all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create address binding on the Switch:

```
DGS-3200-10:4#create address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

59-2 create address_binding ip_mac ipv6address

Purpose

To create an IP-MAC-Port binding entry using IPv6.

Format

create address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}

Description

This command is used to create an IP-MAC-Port binding entry using IPv6.

Parameters

Parameters	Description
<ipv6addr>	Specify the IPv6 address.
mac_address	Specify the MAC address.
ports	Specify to configure a list of ports or all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a static IPv6 IMPB entry that binds the IPv6 address fe80::240:5ff:fe00:28 to the MAC address 00-00-00-00-00-11:

```
DGS-3200-10:4# create address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address
00-00-00-00-00-11
Command: create address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address
00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

59-3 config address_binding ip_mac ports

Purpose

To configure an IP-MAC state to enable or disable for specified ports.

Format

config address_binding ip_mac ports [<portlist> | all] {state [enable {[strict | loose] | [ipv6 | all]} | disable {[ipv6 | all]}] | mode [arp | acl] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable] | stop_learning_threshold <int 0-500> }

Description

This command is used to configure the per port state of IP-MAC binding in the switch.

If a port has been configured as group member of an aggregated link, then it can not enable its IP-MAC binding function. When the binding check state is enabled, for IP packet and ARP packet received by this port, the switch will check whether the IP address and MAC address match the binding entries. The packets will be dropped if they do not match.

For this function, the switch can operate in ACL mode or ARP mode. In ARP mode, only ARP packets are

checked for binding. In ACL mode, both ARP packets and IP packets are checked for the binding. Therefore, ACL mode provides more strict checks for packets.

When configuring the port mode to ACL , the switch will create ACL access entries corresponding to the entries of this port. If the port changes to ARP, all the ACL access entries will be deleted automatically.

Parameters

Parameters	Description
state	Configure the address binding port state to **enable** or **disable**. When this is enabled, the port will perform the binding check.
strict	This mode provides a stricter method of control. If a user chooses it, all packets will be blocked by the Switch by default. The Switch will compare all incoming ARP and IP Packets and attempt to match them against the IMPB white list. If the IP-MAC pair matches the white list entry, the packets from the MAC address will be unblocked. If not the MAC address will remain blocked. While the Strict state uses more CPU resources, from checking every incoming ARP and IP packet, it enforces better security. The default mode is **strict** if not specified.
loose	This mode provides a more loose method of control. If a user chooses this mode, the Switch will forward all packets by default. However, the Switch will still inspect incoming ARP packets and compare them to the Switch's IMPB white list entries. If the IP-MAC pair of a packet is not found in the white list, the Switch will block the MAC address. A major benefit of implementing loose state is that it uses less CPU resources as the Switch only checks incoming packets. However, it is less secure then Strict mode as it cannot block users who only send unicast IP packets. An example of this situation is when a malicious user tries to perform a Denial of Service (DoS) attack by statically configuring the ARP table on their PC. In this case, the Switch cannot block such attacks as the PC will not send out any ARP packets.
ipv6	Specify the IPv6 address.
mode	When configuring the port to ACL mode, the switch will create ACL access entries corresponding to the entries of this port. If the port changes to ARP, all the ACL access entries will be deleted automatically. The default mode of port is ARP mode.

allow_zeroip	Specify whether to allow ARP packets with SIP address 0.0.0.0.. If 0.0.0.0 is not configured in the binding list, when it is set to enabled, the ARP packet with this source IP address 0.0.0.0 will be allowed. When set to disable, this option does not affect the IP-MAC-port binding ACL Mode.
forward_dhcppkt	By default, the DHCP packets with broadcast DA will be flooded. When set to disabled, the broadcast DHCP packets received by the specified port will not be forwarded. This setting is effective when DHCP snooping is enabled because the DHCP packet which has been trapped to CPU needs to be forwarded by the software. This setting controls the forwarding behavior under this situation.
stop_learning_threshold <0-500>	When the number of blocked entries exceeds the threshold, the port will stop learning new addresses. The packet with new addresses will be dropped. The default value is 0 (no limit).

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port 1 to be enabled for address binding:

```
DGS-3200-10:4# config address_binding ip_mac ports 1 state enable
Command: config address_binding ip_mac ports 1 state enable

Success.

DGS-3200-10:4# show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:200
Total Used Rule Entries  :0



Access Profile ID: 1                            Type : IP
================================================================
```

```
Owner     : IP-MAC-PORT Binding
MASK Option :
Source MAC       Source IP MASK
FF-FF-FF-FF-FF-FF  255.255.255.255
-----------------  ---------------

Access ID : 1          Mode: Permit        RX Rate(64Kbps)  : no_limit
Ports    : 1
-----------------  ---------------
00-00-00-00-00-01  10.0.0.1
==============================================================================
Unused Entries: 199



Access Profile ID: 4                               Type : Ethernet
==============================================================================
Owner     : IP-MAC-PORT Binding
MASK Option :
Ethernet Type
-------------

Access ID : 1          Mode: Deny
Ports    : 1
-------------
0x800
==============================================================================
Unused Entries: 199
```

59-4 config address_binding ip_mac ipaddress

Purpose

To update an address binding entry.

Format

config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> {ports [<portlist> | all]}

Description

This command is used to update an address binding entry.

Parameters

Parameters	Description
ipaddr	Specify the IP address.
macaddr	Specify the MAC address.
ports	Configure the portlist to apply. If ports are not configured, it will apply to all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure an address binding entry:

```
DGS-3200-10:4#config address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address
00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

59-5 config address_binding ip_mac ipv6address

Purpose

To update an address binding entry using IPv6.

Format

config address_binding ip_mac ipv6address <ipv6addr> mac_address <macaddr> {ports [<portlist> | all]}

Description

This command is used to update an address binding entry using IPv6.

Parameters

Parameters	Description
ipv6address	Specify the IPv6 address used.
macaddr	Specify the MAC address.
ports	Specify the portlist to apply. If ports are not configured, it will apply to all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a static IPv6 IMPB entry so that that IPv6 address fe80::240:5ff:fe00:28 is bound to the MAC address 00-00-00-00-00-11:

```
DGS-3200-10:4# config address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipv6address fe80::240:5ff:fe00:28
mac_address 00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

59-6 delete address_binding blocked

Purpose

To delete a blocked entry.

Format

delete address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Description

This command is used to delete a blocked entry. It specifies the address database that the system has automatically learned and blocked.

Parameters

Parameters	Description
all	Specify that all the blocked MAC addresses will be used.
vlan_name	Specify the name of the VLAN that the blocked MAC address belongs to.
mac_address	Specify the MAC address of the blocked MAC address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete the blocked MAC address 00-00-00-00-00-11, which belongs to the VLAN named “v31”:

```
DGS-3200-10:4# delete address_binding blocked vlan_name v31 mac_address
00-00-00-00-00-11
Command: delete address_binding blocked vlan_name v31 mac_address 00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

59-7 delete address_binding ip_mac

Purpose

To delete an IMPB entry.

Format

delete address_binding ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>| ipv6address <ipv6addr> mac_address <macaddr>]

Description

This command is used to delete an IMPB entry.

Parameters

Parameters	Description
all	Specify that all the MAC addresses will be used.
ipaddress	Specify the learned IP address of the entry in the database.
ipv6address	Specify the learned IPv6 address of the entry in the database.
mac_address	Specify the MAC address of the entry or the blocked MAC address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete an IMPB entry that binds the IP address 10.1.1.1.1 to the MAC address 00-00-00-00-00-11:

```
DGS-3200-10:4# delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

To delete a static ipv6 IMPB entry that binds the IPv6 address fe80::240:5ff:fe00:28 to the MAC address

00-00-00-00-00-11:

```
DGS-3200-10:4# delete address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address
00-00-00-00-00-11
Command: delete address_binding ip_mac ipv6address fe80::240:5ff:fe00:28 mac_address
00-00-00-00-00-11

Success.

DGS-3200-10:4#
```

59-8 show address_binding

Purpose

To display address binding entries, blocked MAC entries, and port status.

Format

show address_binding {ports {<portlist>}}

Description

This command is used to display address binding information.

Parameters

Parameters	Description
ports	Specify a list of ports to display the state of the IP-MAC-Port Binding.

Restrictions

None.

Examples

To display the address binding global configuration:

```
DGS-3200-10:4#show address_binding
Command: show address_binding

Trap/Log          : Disabled
DHCP Snoop(IPv4)  : Disabled
DHCP Snoop(IPv6)  : Disabled
ND Snoop          : Disabled
Function Version  : 3.82



DGS-3200-10:4#
```

To display the address binding global configuration by port:

```
DGS-3200-10:4#show address_binding ports
Command: show address_binding ports

 Port   IPv4       IPv6       Mode  Zero IP    DHCP Packet  Stop Learning
        State      State                                     Threshold/Mode
 -----  ---------  ---------  ----  ---------  -----------  --------------
 1      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 2      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 3      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 4      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 5      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 6      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 7      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 8      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 9      Disabled   Disabled   ARP   Not Allow  Forward      500/Normal
 10     Disabled   Disabled   ARP   Not Allow  Forward      500/Normal


DGS-3200-10:4#
```

59-9 show address_binding blocked

Purpose

To display address binding information for blocked entries.

Format

show address_binding blocked [all | vlan_name <vlan_name> mac_address <macaddr>]

Description

This command is used to display address binding information for blocked entries.

Parameters

Parameters	Description
all	Specify to display all.
vlan_name	Specify the VLAN name that the blocked MAC belongs to.
mac_address	Specify the MAC address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To show the IMPB entries that are currently blocked:

```
DGS-3200-10:4# show address_binding blocked all
Command: show address_binding blocked all

 VID  VLAN Name                    MAC Address      Port
 ---- ------------------------------ ----------------- ----
 1    default                     00-01-02-03-29-38  7
 1    default                     00-0C-6E-5C-67-F4  7
 1    default                     00-0C-F8-20-90-01  7
 1    default                     00-0E-35-C7-FA-3F  7
 1    default                     00-0E-A6-8F-72-EA  7
 1    default                     00-0E-A6-C3-34-BE  7
 1    default                     00-11-2F-6D-F3-AC  7
 1    default                     00-50-8D-36-89-48  7
 1    default                     00-50-BA-00-05-9E  7
 1    default                     00-50-BA-10-D8-F6  7
 1    default                     00-50-BA-38-7D-E0  7
 1    default                     00-50-BA-51-31-62  7
 1    default                     00-50-BA-DA-01-58  7
 1    default                     00-A0-C9-01-01-23  7
 1    default                     00-E0-18-D4-63-1C  7

Total Entries : 15

DGS-3200-10:4#
```

59-10 show address_binding ip_mac

Purpose

To display the user created database of address binding information.

Format

show address_binding ip_mac [all | [[ipaddress <ipaddr> | ipv6address <ipv6addr>] {mac_address <macaddr>} | mac_address <macaddr>]]

Description

This command is used to display the user created database of address binding information.

Parameters

Parameters	Description
all	Specify to display all.
ipaddress	Specify the IP address.
ipv6address	Specify the IPv6 address.
mac_address	Specify the MAC address.

Restrictions

None.

Examples

To display all the IP-MAC address binding information:

```
DGS-3200-10:4# show address_binding ip_mac all
Command: show address_binding ip_mac all

 M(Mode) - D:DHCP, N:ND S:Static ACL - A:Active I:Inactive

 IP Address                        MAC Address      M  ACL Ports
 ------------------------------------ ----------------- -- -- ---------------
 10.1.1.1                          00-11-22-33-44-55 S  I  1
 10.1.1.2                          00-22-33-44-55-66 S  A  2
 2001::1                           00-33-44-55-66-77 S  I  3

Total Entries : 3

DGS-3200-10:4#
```

59-11 enable address_binding trap_log

Purpose

To enable an address binding trap/log.

Format

enable address_binding trap_log

Description

This command is used to send trap and log messages when an address binding module detects illegal IP

and MAC addresses.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable an address binding trap log:

```
DGS-3200-10:4#enable address_binding trap_log
Command: enable address_binding trap_log


Success.


DGS-3200-10:4#
```

59-12 disable address_binding trap_log

Purpose

To disable the address binding trap/log.

Format

disable address_binding trap_log

Description

This command is used to disable address binding trap logs.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the address binding trap log:

```
DGS-3200-10:4#disable address_binding trap_log
Command: disable address_binding trap_log


Success.


DGS-3200-10:4#
```

59-13 enable address_binding dhcp_snoop

Purpose

To enable the address binding DHCP snooping mode.

Format

enable address_binding dhcp_snoop {[ipv6 | all]}

Description

This command is used to enable the address binding mode. By default, DHCP snooping is disabled.
If a user enables DHCP snooping, all address binding disabled ports will function as server ports (the switch will learn IP addresses through server ports (by DHCP OFFER and DHCP ACK packets)).

The auto-learned IP-MAC binding entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an ACL-mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time expires, the expired entry will be removed from this port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address has moved to a different port.

Consider the case in which a binding entry learned by DHCP snooping conflicts with the statically configured entry. This means that the binding relation is in conflict. For example, if IP A is binded with MAC X by static configuration, suppose that the binding entry learned by DHCP snooping is IP A binded by MAC Y, then there is a conflict. When the DHCP snooping learned entry is binded with the static configured entry, then the DHCP snooping learned entry will not be created.

Consider the other conflict case, when the DHCP snooping learned a binding entry, and the same IP-MAC binding pair has been statically configured. If the learned information is consistent with the statically configured entry, then the auto-learned entry will not be created. If the entry is statically configured in ARP mode, then the auto learned entry will not be created. If the entry is statically configured on one port and the entry is auto-learned on another port, then the auto-learned entry will not be created either.

Parameters

Parameters	Description
ipv6	Specify that the address used is an IPv6 address.
all	Specify that all IP addresses will be used.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the address binding auto mode:

```
DGS-3200-10:4#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3200-10:4#
```

59-14 disable address_binding dhcp_snoop

Purpose

To disable the address binding DHCP snooping mode.

Format

disable address_binding dhcp_snoop {[ipv6 | all]}

Description

When this is disabled, all of the auto-learned binding entries will be removed.

Parameters

Parameters	Description
ipv6	Specify that the address used is an IPv6 address.
all	Specify that all IP addresses will be used.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the address binding auto mode:

```
DGS-3200-10:4#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3200-10:4#
```

59-15 enable address_binding nd_snoop

Purpose

To enable ND snooping on the Switch.

Format

enable address_binding nd_snoop

Description

This command is used to enable ND snooping on the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the ND snooping function on the Switch:

```
DGS-3200-10:4# enable address_binding nd_snoop
Command: enable address_binding nd_snoop


Success.


DGS-3200-10:4#
```

59-16 disable address_binding nd_snoop

Purpose

To disable ND snooping on the switch.

Format

disable address_binding nd_snoop

Description

This command allows the user to disable ND Snooping on switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the ND snooping function on the Switch:

```
DGS-3200-10:4# disable address_binding nd_snoop
Command: disable address_binding nd_snoop

Success.

DGS-3200-10:4#
```

59-17 config address_binding nd_snoop ports

Purpose

To specify the maximum number of entries that can be learned with ND snooping.

Format

config address_binding nd_snoop ports [< portlist > | all] max_entry [< value 1-10 > | no_limit]

Description

This command specifies the maximum number of entries that a port can learn with ND snooping.

Parameters

Parameters	Description
ports	**<portlist>** - Specify the list of ports that require a restriction on the the maximum number of entries that can be learned with ND snooping. **all** - Specify all the ports on the switch.
max_entry	Specify the maximum number of entries.
no_limit	Specify that the maximum number of learned entries is unlimited.

Restrictions

Only Administrator-level users can issue this command.

Examples

To specify that a maximum of 10 entries can be learned by ND snooping on ports 1-3:

```
DGS-3200-10:4# config address_binding nd_snoop ports 1-3 max_entry 10
Command: config address_binding nd_snoop ports 1-3 max_entry 10

Success.

DGS-3200-10:4#
```

59-18 show address_binding nd_snoop

Purpose

To display the status of ND snooping on the switch.

Format

show address_binding nd_snoop {ports <portlist>}

Description

This command is used to display the status of ND snooping on the switch.

Parameters

Parameters	Description
ports	Specify the ports to display the ND Snooping information. If no parameter is specified, the ND Snooping information will be displayed for all ports.

Restrictions

None.

Examples

To show the ND snooping state:

```
DGS-3200-10:4# show address_binding nd_snoop
Command: show address_binding nd_snoop

ND Snoop     : Enabled

DGS-3200-10:4#
```

To show the ND snooping maximum entry information for ports 1-5:

```
DGS-3200-10:4#show address_binding nd_snoop  ports 1-5
Command: show address_binding nd_snoop ports 1-5

Port  Max Entry
----  ---------
1     No Limit
2     No Limit
3     No Limit
4     No Limit
5     No Limit

DGS-3200-10:4#
```

59-19 show address_binding nd_snoop binding_entry

Purpose

To display the ND snooping binding entries on the switch.

Format

show address_binding nd_snoop binding_entry {port <port>}

Description

This command is used to show the ND snooping binding entries on the switch.

Parameters

Parameters	Description
port	Specify a port to display. If no parameter is specified, it will show all ND snooping binding entries.

Restrictions

None.

Examples

To display the ND snooping binding entry:

```
DGS-3200-10:4# show address_binding nd_snoop binding_entry
Command: show address_binding nd_snoop binding_entry

S (Status) - A: Active, I: Inactive
Time - Left Time (sec)
IP Address                                MAC Address        S  LT(sec)  Port
----------------------------------------- ------------------ -- -------- ----
```

```
2001:2222:1111:7777:5555:6666:7777:8888   00-00-00-00-00-02  I  50        5
2001::1                                    00-00-00-00-03-02  A  100       6

Total Entries : 2

DGS-3200-10:4#
```

59-20 clear address_binding dhcp_snoop

Purpose

To clear the address binding entries learned for the specified ports.

Format

clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {[ipv6 | all]}

Description

This command is used to clear the address binding entries learned for the specified ports.

Parameters

Parameters	Description
ports	Specify the list of ports to clear the DHCP-snoop learned entry.
all	Specify all ports.
ipv6	Specify that the address used is an IPv6 address. Specify all to use all IPv6 addresses.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the address binding entries for ports 1 to 3:

```
DGS-3200-10:4# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3200-10:4#
```

59-21 clear address_binding nd_snoop binding_entry

Purpose

To clear the ND snooping entries on specified ports.

Format

clear address_binding nd_snoop binding_entry ports [<portlist> | all]

Description

This command is used to clear the ND snooping entries on specified ports.

Parameters

Parameters	Description
ports	Specify the list of ports that you would like to clear the ND snoop learned entry.
all	Clear all ND snooping learned entries.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the ND snooping entries on ports 1-3:

```
DGS-3200-10:4# clear address_binding nd_snoop binding_entry ports 1-3
Command: clear address_binding nd_snoop binding_entry ports 1-3

Success.

DGS-3200-10:4#
```

59-22 show address_binding dhcp_snoop

Purpose

To show the address binding auto learning databases.

Format

show address_binding dhcp_snoop {max_entry {ports <portlist>}}

Description

This command is used to display all the auto-learning databases.

Parameters

Parameters	Description

max_entry	Specify to display the maximum number of entries.
ports	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display address binding DHCP snooping:

```
DGS-3200-10:#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP Snoop(IPv4) : Enabled
DHCP Snoop(IPv6) : Disabled

DGS-3200-10:4#
```

To display the address binding DHCP snooping maximum entries on port 1 to 10:

```
DGS-3200-10:# show address_binding dhcp_snoop max_entry ports 1-10
Command: show address_binding dhcp_snoop max_entry ports 1-10

Port  Max Entry  Max IPv6 Entry
----  ---------  --------------
1     No Limit   No Limit
2     10         No Limit
3     20         No Limit
4     No Limit   No Limit
5     No Limit   No Limit
6     No Limit   No Limit
7     No Limit   No Limit
8     No Limit   No Limit
9     No Limit   No Limit
10    No Limit   No Limit

DGS-3200-10:4#
```

59-23 config address_binding dhcp_snoop max_entry

Purpose

To specify the maximum number of entries which can be learned by the specified ports.

Format

config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit] {ipv6}

Description

This command is used to specify the maximum number of entries which can be learned by the specified ports. By default, the per port maximum entry is no limit.

Parameters

Parameters	Description
portlist	Specify the list of ports to clear the DHCP-snooping learned entry.
limit	Specify the maximum number.
ipv6	Specify that the configuration is for IPv6 DHCP Snooping.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the maximum number of entries that ports 1 to 3 can learn to 10:

```
DGS-3200-10:4#config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DGS-3200-10:4#
```

59-24 show address_binding dhcp_snoop binding_entry

Purpose

To display DHCP snooping information of a specific binding entry.

Format

show address_binding dhcp_snoop binding_entry {port <port>}

Description

This command is used to display DHCP snooping information of a specific binding entry.

Parameters

Parameters	Description
port	Specify a port on which to display the binding entry.

Restrictions

None.

Examples

To display the DHCP snooping binding entries:

```
DGS-3200-10:4# show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

 S (Status) - A: Active, I: Inactive
 Time - Left Time (sec)

 IP Address                       MAC Address      S  LT(sec)   Port
 ---------------------------------- ----------------- -- ---------- -----
 10.62.58.35                       00-0B-5D-05-34-0B A  35964     1
 10.33.53.82                       00-20-c3-56-b2-ef I  2590      2
 2001:2222:1111:7777:5555:6666:7777:8888 00-00-00-00-00-02 I  50       5
 2001::1                          00-00-00-00-03-02 A  100       6

Total entries : 4

DGS-3200-10:4#
```

59-25 config address_binding recover_learning ports

Purpose

To unfreeze the ARP check for ports.

Format

config address_binding recover_learning ports [<portlist> | all]

Description

This command is used to recover the ARP check function if it has ceased to work.

Parameters

Parameters	Description
portlist	Specify the list of ports to clear the DHCP-snooping learned entry.

Restrictions

Only Administrator-level users can issue this command.

Examples

To unfreeze the ARP check for ports 6 and 7 :

```
DGS-3200-10:4# config address_binding recover_learning ports 6-7
Command: config address_binding recover_learning ports 6-7


Success.


DGS-3200-10:4#
```

60 Web-based Access Control Command List

enable wac
disable wac
config wac authorization attributes {radius [enable | disable] local [enable | disable]}
config wac ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}
config wac method [local | radius]
config wac default_redirpath <string 128>
config wac clear_default_redirpath
config wac virtual_ip <ipaddr>
config wac switch_http_port <tcp_port_number 1-65535> { [http | https] }
create wac user <username 15> { [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] }
delete wac [user <username 15> | all_users]
config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094> | clear_vlan]
show wac
show wac ports {<portlist>}
show wac user
show wac auth_state ports {<portlist>}
clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr> }]
config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title < desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]
show wac authenticate_page

60-1 enable wac

Purpose

To enable the Web-based Access Control function.

Format

enable wac

Description

This command is used to enable the WAC function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the WAC function:

```
DGS-3200-10:4# enable wac
Command: enable wac

Success.

DGS-3200-10:4#
```

60-2 disable wac

Purpose

To disable the Web-based Access Control function.

Format

disable wac

Description

This command is used to disable the WAC function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the WAC function:

```
DGS-3200-10:4# disable wac
Command: disable wac

Success.

DGS-3200-10:4#
```

60-3 config wac authorization attributes

Purpose

To configure the acceptance of an authorized configuration.

Format

config wac authorization attributes {radius [enable | disable] local [enable | disable]}

Description

This command is used to configure the acceptance of an authorized configuration. When the authorization is enabled for WAC's RADIUS, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. When the authorization is enabled for WAC's local, the authorized data assigned by the local database will be accepted.

Parameters

Parameters	Description
radius	If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. The default state is enabled.
local	If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the acceptance of an authorized configuration:

```
DGS-3200-10:4# config wac authorization attributes local disable
Command: config wac authorization attributes local disable

Success.

DGS-3200-10:4#
```

60-4 config wac ports

Purpose

To configure the WAC port level setting.

Format

config wac ports [<portlist> | all] {state [enable | disable] | | aging_time [infinite | <min 1-1440>] |

idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}

Description

This command is used to configure the Web authentication setting.

Parameters

Parameters	Description
state	Specify to enable or disable WAC state.
aging_time	A time period during which an authenticated host will be kept in authenticated state. **infinite** indicates the authenticated host on the port will not age out. The default value is 24 hours.
idle_time	A time period after which an authenticated host will be moved to un-authenticated state if there is no traffic during that period. **infinite** indicates the host will not be removed from the authenticated state due to idle of traffic. The default value is **infinite**.
block_time	If a host fails to pass the authentication, it will be blocked for this period of time before it can be re-authenticated. The default value is 60 seconds.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the WAC port state:

```
DGS-3200-10:4# config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

DGS-3200-10:4#
```

To configure port aging time:

```
DGS-3200-10:4# config wac ports 1 aging_time 10
Command: config wac ports 1 aging_time 10

Success.

DGS-3200-10:4#
```

60-5 config wac

Purpose

To configure the Web authentication global parameters.

Format

config wac method [local | radius]

Description

This command is used to configure the global parameters for Web authentication.

Parameters

Parameters	Description
method	Specify the authenticated method
local	The authentication will be done via the local database.
radius	The authentication will be done via the RADIUS server.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the authentication method:

```
DGS-3200-10:4# config wac method radius
Command: config wac method radius

Success.

DGS-3200-10:4#
```

60-6 config wac default_redirpath

Purpose

To configure the WAC default redirect path.

Format

config wac default_redirpath <string 128>

Description

This command is used to configure the WAC default redirect path. If default redirect path is configured, the user will be redirected to the default redirect path after successful authentication. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Parameters

Parameters	Description
<string 128>	The URL that the client will be redirected to after successful authentication. By default, the redirected path is cleared

Restrictions

Only Administrator-level users can issue this command.

Example

To configure WAC default redirect path:

```
DGS-3200-10:config wac default_redirpath http://www.dlink.com
Command: config wac default_redirpath http://www.dlink.com

Success.

DGS-3200-10:
```

60-7 config wac clear_default_redirpath

Purpose

To clear WAC default redirect path.

Format

config wac clear_default_redirpath

Description

This command is used to clear a WAC default redirect path. When the string is cleared, the client will not be redirected to another URL after successful authentication.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear a WAC default redirect path:

```
DGS-3200-10:4#config wac clear_default_redirpath
Command: config wac clear_default_redirpath

Success.

DGS-3200-10:4#
```

60-8 config wac virtual_ip

Purpose

To configure the WAC virtual IP address used to accept authentication requests from unauthenticated hosts.

Format

config wac virtual_ip <ipaddr>

Description

This command is used to configure the WAC virtual IP address. When virtual IP is specified, the TCP packets sent to the virtual IP will get a reply. If virtual IP is enabled, TCP packets sent to the virtual IP or physical IPIF's IP address will both get the reply. When virtual IP is set 0.0.0.0, the virtual IP will be disabled. By default, the virtual IP is 0.0.0.0. The virtual IP will not respond to any ARP requests or ICMP packets. To make this function work properly, the virtual IP should not be an existing IP address. It also cannot be located on an existing subnet.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the virtual IP.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the WAC virtual IP address used to accept authentication requests from unauthenticated hosts:

```
DGS-3200-10:4# config wac virtual_ip 1.1.1.1
Command: config wac virtual_ip 1.1.1.1

Success.

DGS-3200-10:4#
```

60-9 config wac switch_http_port

Purpose

To configure the TCP port which the WAC switch listens to.

Format

config wac switch_http_port < tcp_port_number 1-65535> {[http | https]}

Description

This command is used to configure the TCP port which the WAC switch listens to. The TCP port for HTTP or HTTPs is used to identify the HTTP or HTTPs packets that will be trapped to CPU for authentication processing, or to access the login page. If not specified, the default port number for HTTP is 80, and the default port number for HTTPS is 443. If no protocol is specified, the protocol is HTTP.

Parameters

Parameters	Description
<tcp_port_number 1-65535>	A TCP port which the WAC switch listens to and uses to finish the authenticating process.
http	Specify that WAC runs HTTP protocol on this TCP port.
https	Specify that WAC runs HTTPS protocol on this TCP port.

Restrictions

The HTTP cannot run at TCP port 443, and the HTTPS cannot run at TCP port 80. Only Administrator-level users can issue this command.

Example

To configure a TCP port which the WAC switch listens to:

```
DGS-3200-10:4# config wac switch_http_port 8888 http
Command: config wac switch_http_port 8888 http

Success.

DGS-3200-10:4#
```

60-10 create wac user

Purpose

To create user accounts for Web-based Access Control.

Format

create wac user <username 15> {[vlan <vlan_name 32> | vlanid <vlanid 1-4094>]}

Description

This command is used to create accounts for Web-based Access Control. This user account is independent of the login user account. If VLAN is not specified, the user will not get a VLAN assigned after the authentication.

Parameters

Parameters	Description
username	User account for Web-based Access Control.
vlan	The authentication VLAN name.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a WAC account:

```
DGS-3200-10:4#create wac user dk vlan default
Command: create wac user dk vlan default

Enter a case-sensitive new password:**
Enter the new password again for confirmation:**
Success.

DGS-3200-10:4#
```

60-11 delete wac user

Purpose

To delete a Web-based Access Control account.

Format

delete wac [user <username 15> | all users]

Description

This command is used to delete an account.

Parameters

Parameters	Description
username	User account for Web-based Access Control.
all users	Select this option to delete all current WAC users.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a WAC account:

```
DGS-3200-10:4#delete wac user dk
Command: delete wac user dk

Success.

DGS-3200-10:4#
```

60-12 config wac user

Purpose

To configure the VLAN ID of the user account.

Format

config wac user <username 15> [vlan <vlan_name 32> | vlanid <vlanid 1-4094>| clear_vlan]

Description

This command is used to change the VLAN associated with a user.

Parameters

Parameters	Description
username	The name of user account which will change its VID.
vlan	The authentication VLAN name.
clear_vlan	Choose to clear the specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the port state:

```
DGS-3200-10:4# config wac user duhon vlan default
Command: config wac user duhon vlan default

Enter a old password:*
Enter a case-sensitive new password:***
Enter the new password again for confirmation:***
Success.
```

```
DGS-3200-10:4#
```

60-13 show wac

Purpose

To display the Web authentication global setting.

Format

show wac

Description

This command is used to display the Web authentication global setting.

Parameters

None.

Restrictions

None.

Examples

To show WAC:

```
DGS-3200-10:4#show wac
Command: show wac

 Web-based Access Control
 --------------------------------
 State                : Enabled
 Method               : RADIUS
 Redirect Path         : http://www.dlink.com
 Virtual IP           : 0.0.0.0
 Switch HTTP Port      : 80 (HTTP)
 RADIUS Authorization   : Enabled
 Local Authorization    : Enabled

DGS-3200-10:4#
```

60-14 show wac ports

Purpose

To display the Web authentication port level setting.

Format

show wac ports {<portlist>}

Description

This command is used to display the port level setting.

Parameters

Parameters	Description
ports	A range of member ports to show the status.

Restrictions

None.

Examples

To show WAC ports 1 to 3:

```
DGS-3200-10:4#show wac ports  1-3
Command: show wac ports 1-3

 Port    State         Aging Time    Idle Time       Block Time
                          (min)         (min)           (sec)
 -----  --------    -------------  -------------  -------------
 1      Enabled     10             Infinite       60
 2      Enabled     1440           Infinite       60
 3      Enabled     1440           Infinite       60

DGS-3200-10:4#
```

60-15 show wac user

Purpose

To display Web authentication user accounts.

Format

show wac user

Description

This command is used to display Web authentication accounts.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To show Web authentication user accounts:

```
DGS-3200-10:4#show wac user
Command: show wac user

 User Name           Password            VID
 ----------------  ----------------  ---------
   dk                  dk                  1
   dlink               dlink               -

 Total Entries:2



DGS-3200-10:4#
```

60-16 show wac auth_state

Purpose

To display the authentication state of a port.

Format

show wac auth_state ports {<portlist>}

Description

This command is used to display the authentication state for ports.

Parameters

Parameters	Description
ports	Specify the list of ports whose WAC state will be displayed.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the port authentication status of ports 13:

```
DGS-3200-10:4# show wac auth_state ports 1-3
Command: show wac auth_state ports 1-3

P:Port-based   Pri:Priority

Port    MAC Address       Original  State       VID Pri Aging Time/ Idle
                            RX VID                      Block Time  Time
------ ------------------- ---- -------------- ---- -- ----------- ----
1       00-00-00-00-00-01    20   Authenticated  -    3  Infinite    40
1       00-00-00-00-00-02    20   Authenticated  1234 -  Infinite    50
1       00-00-00-00-00-03    100  Blocked        -    -  60           -
1       00-00-00-00-00-04    110  Authenticating -    -  10           -
2       00-00-00-00-00-10(P) 2040 Authenticated  1234 2  1440        20
3       00-00-00-00-00-20(P) 2045 Authenticating -    -  5            -
3       00-00-00-00-00-21    2041 Blocked        -    6  1100        80

 Total Authenticating Hosts  : 2
 Total Authenticated Hosts   : 3
 Total Blocked Hosts         : 2
DGS-3200-10:4#
```

60-17 clear wac auth_state

Purpose

To clear the WAC authentication state of a port.

Format

clear wac auth_state [ports [<portlist> | all] {authenticated | authenticating | blocked} | macaddr <macaddr> }]

Description

This command is used to clear the authentication state of a port. The port will return to un-authenticated state. All the timers associated with the port will be reset.

Parameters

Parameters	Description
ports	Specify the list of ports whose WAC state will be cleared.
authenticated	Specify to clear all authenticated users for a port.
authenticating	Specify to clear all authenticating users for a port.
blocked	Specify to clear all blocked users for a port.

macaddr	Specify to clear a specific user.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear the WAC state of ports 1 to 5:

```
DGS-3200-10:4# clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DGS-3200-10:4#
```

60-18 config wac authentication_page element

Purpose

To customize the authenticate page elements.

Format

config wac authentication_page element [default | page_title <desc 128> | login_window_title <desc 64> | user_name_title < desc 32> | password_title <desc 32> | logout_window_title <desc 64> | notification_line <value 1-5> <desc 128>]

Description

This command is used to customize the authenticate page elements.

Parameters

Parameters	Description
default	Specify to reset the page elements to default.
page_title	Specify to configure the title of the authentication page.
login_window_title	Specify to configure the login window title of the authentication page.
user_name_title	Specify to configure the user name title of the authentication page.
password_title	Specify to configure the password title of the authentication page.
logout_window_title	Specify to configure the logout window title of the authentication page.
notification_line	Specify to set the notification information by line in authentication Web pages.

Restrictions

Only Administrator-level users can issue this command.

Examples

To customize the authenticate page elements:

```
DGS-3200-10:4# config wac authentication_page element notification_line 1 Copyright @ 2011 D-Link
All Rights Reserved
Command: config wac authentication_page element notification_line 1 Copyright @ 2011 D-Link All
Rights Reserved

Success.

DGS-3200-10:4#
```

60-19 show wac authenticate_page

Purpose

To show the elements of the customized authenticate pages.

Format

show wac authenticate_page

Description

This command is used to show the elements of the customized authenticate pages.

Parameters

None.

Restrictions

None.

Examples

The following example displays the authentication page elements:

```
DGS-3200-10:4# show wac authenticate_page
Command: show wac authenticate_page

Page Title                      : D-Link
Login Window Title              : Authentication Login
User Name Title                 : User Name
Password Title                  : Password
Logout Window Title             : Logout
```

```
Notification                    :

Copyright @ 2011 D-Link All Rights Reserved

Site: http://support.dlink.com


DGS-3200-10:4#
```

61 MAC-based Access Control Command Lists

enable mac_based_access_control
disable mac_based_access_control
config mac_based_access_control password <passwd 16>
config mac_based_access_control method [local | radius]
config mac_based_access_control guest_vlan ports <portlist>
config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1 - 4096> | no_limit]}
create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid < vlanid 1-4094>]
clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]
create mac_based_access_control_local mac <macaddr> {[vlan <vlan_name 32> | vlanid < vlanid 1-4094>]}
config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid < vlanid 1-4094>| clear_vlan]
config mac_based_access_control max_users [<value 1 - 4096> |no_limit]
config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}
delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid < vlanid 1-4094>]
show mac_based_access_control auth_state ports {<portlist>}
show mac_based_access_control {ports {<portlist>}}
show mac_based_access_control_local {[mac<macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]}
config mac_based_access_control log state [enable | disable]
config mac_based_access_control trap state [enable | disable]
config mac_based_access_control password_type [manual_string | client_mac_address]

61-1 enable mac_based_access_control

Purpose

To enable MAC-based Access Control.

Format

enable mac_based_access_control

Description

This command is used to enable the MAC-based Access Control function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable MAC-based Access Control:

```
DGS-3200-10:4# enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3200-10:4#
```

61-2 disable mac_based_access_control

Purpose

To disable MAC-based Access Control.

Format

disable mac_based_access_control

Description

This command is used to disable the MAC-based Access Control function.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable MAC-based Access Control:

```
DGS-3200-10:4# disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3200-10:4#
```

61-3 config mac_based_access_control password

Purpose

To configure the password of the MAC-based Access Control.

Format

config mac_based_access_control password <passwd 16>

Description

This command is used to set the password that will be used for authentication via RADIUS server.

Parameters

Parameters	Description
<passwd 16>	In RADIUS mode, the switch communicates with the RADIUS server using this password. The maximum length of the key is 16.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the password “rosebud” that will be used for authentication via RADIUS server:

```
DGS-3200-10:4# config mac_based_access_control password rosebud
Command: config mac_based_access_control password rosebud

Success.

DGS-3200-10:4#
```

61-4 config mac_based_access_control method

Purpose

To configure the MAC-based Access Control authenticating method.

Format

config mac_based_access_control method [local | radius]

Description

This command is used to authenticate via a local database or a RADIUS server.

Parameters

Parameters	Description
local	Specify to authenticate via local database.
radius	Specify to authenticate via RADIUS server.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MAC-based Access Control method as local:

```
DGS-3200-10:4# config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3200-10:4#
```

61-5 config mac based_access_control guest_vlan

Purpose

To configure the MAC-based Access Control guest VLAN membership.

Format

config mac_based_access_control guest_vlan ports <portlist>

Description

This command is used to put the specified port in guest VLAN mode. For those ports not contained in the port list, they are in non-guest VLAN mode. For detailed information about the operation of guest VLAN mode, please see the description for configuring the MAC-based Access Control port command.

Parameters

Parameters	Description
<portlist>	When the guest VLAN is configured for a port, the port will do the VLAN assignment based on the assigned VLAN from the RADIUS server. When the guest VLAN is not configured, the port will not do the VLAN assignment.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MAC-based Access Control guest VLAN membership for port 1 to 8:

```
DGS-3200-10:4# config mac_based_access_control guest_vlan ports 1-8
Command: config mac_based_access_control guest_vlan ports 1-8

Success.

DGS-3200-10:4
```

61-6 config mac_based_access_control ports

Purpose

To configure the MAC-based Access Control parameters.

Format

config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | aging_time [infinite | <min 1-1440>] | block_time <sec 0-300> | max_users [<value 1 - 4096> | no_limit]}

Description

This command is used to configure the MAC-based Access Control setting. When the MAC-AC function is enabled for a port, and the guest VLAN function for this port is disabled, the user attached to this port will not be forwarded unless the user passes the authentication. The user that does not pass the authentication will not be serviced by the switch. If the user passes the authentication, the user will be able to forward traffic operated under the original VLAN configuration. When the MAC-AC function is enabled for a port, and the guest VLAN function for this port is enabled, it will move from the original VLAN member port, and become a member port of the guest VLAN before the authentication process starts. After the authentication, if a valid VLAN is assigned by the RADIUS server, this port will then be removed from the guest VLAN and become a member port of the assigned VLAN.

For guest VLAN mode, there are two situations that need to be considered. If a device supports port-based VLAN classification only, when the port has been moved to the authorized VLAN, the subsequent users will not be authenticated again. They will operate in the current authorized VLAN. If the device supports MAC-based VLAN classification, then each user will be authorized individually and will be capable of getting its own VLAN.

For guest VLAN mode, if the MAC address is authorized, but no VLAN information is assigned from a RADIUS Server or the VLAN assigned by RADIUS server is invalid (e.g. the assigned VLAN does not

exist), this port/MAC will be removed from member port of the guest VLAN and it will become a member port of the original VLAN.

Parameter

Parameters	Description
ports	A range of ports to enable or disable the MAC-based Access Control function.
state	Specify whether the MAC AC function is enabled or disabled.
aging_time	A time period during which an authenticated host will be kept in the authenticated state. When the aging time is timed-out, the host will be moved back to unauthenticated state.
block_time	If a host fails to pass the authentication, the next authentication will not start within the block time unless the user clears the entry state manually. If the block time is set to 0, it means that clients that fail authentication will not be blocked.
max_users	Specify maximum number of users per port. Specify **no_limit** for not limiting the maximum number of users on the port.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the MAC-based Access Control authorization maximum number for ports 1 to 8:

```
DGS-3200-10:4# config mac_based_access_control ports 1-8 max_users 100
Command: config mac_based_access_control ports 1-8 max_users 100

Success

DGS-3200-10:4#
```

61-7 create mac_based_access_control guest_vlan

Purpose

To assign a guest VLAN.

Format

create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <1-4094>]

Description

This command is used to assign a guest VLAN.

Parameters

Parameters	Description
guest_vlan	If the MAC address is authorized, the port will be assigned to this VLAN.
guest_vlanid	If the MAC address is authorized, the port will be assigned to this VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a MAC local:

```
DGS-3200-10:4# create mac_based_access_control 1 guest_vlanid 2
Command: create mac_based_access_control 1 guest_vlanid 2

Success.

DGS-3200-10:4#
```

61-8 delete mac_based_access_control guest_vlan

Purpose

To de-assign a guest VLAN.

Format

delete mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <1-4094>]

Description

This command is used to de-assign a guest VLAN. When a guest VLAN is de-assigned, the guest VLAN function is disabled.

Parameters

Parameters	Description
guest_vlan	Delete database with this VLAN name.
guest_vlanid	Delete database with this VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Examples

To de-assign a guest VLAN:

```
DGS-3200-10:4# delete mac_based_access_control guest_vlan default
```

```
Command: delete mac_based_access_control guest_vlan default

Success.

DGS-3200-10:4#
```

61-9 clear mac_based_access_control auth_state

Purpose

To clear the authentication state of a user (or port).

Format

clear mac_based_access_control auth_state [ports [all | <portlist>] | mac_addr <macaddr>]

Description

This command is used to clear the authentication state of a user (or port). The port (or the user) will return to un-authenticated state. All the timers associated with the port (or the user) will be reset.

Parameters

Parameters	Description
ports	Specify the port range to clear the authentication state.
mac_addr	Specify to clear a specified host authentication state.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear the authentication state of all ports:

```
DGS-3200-10:4# clear mac_based_access_control auth_state ports all
Command: clear mac_based_access_control auth_state ports all

Success.

DGS-3200-10:4#
```

61-10 create mac_based_access_control_local

Purpose

To create the local database entry.

Format

create mac_based_access_control_local mac <macaddr> {[vlan < vlan_name 32> | vlanid <1-4094>]}

Description

This command is used to create a database entry.

Parameters

Parameters	Description
mac	The MAC address that access accepts by local mode.
vlan	If the MAC address is authorized, the port will be assigned to this VLAN.
vlanid	If the MAC address is authorized, the port will be assigned to this VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a local database entry:

```
DGS-3200-10:4# create mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3200-10:4#
```

61-11 config mac_based_access_control max_users

Purpose

To configure the MAC-based access control maximum number of authorized users.

Format

config mac_based_access_control max_users [<value 1 - 4096> |no_limit]

Description

This command is used to configure the MAC-based access control maximum number of authorized users.

Parameters

Parameters	Description
<value 1-4096>	Specify the maximum number of authorized users.
no_limit	Specify to have unlimited number of authorized users.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the MAC-based access control maximum number of authorized users:

```
DGS-3200-10:4# config mac_based_access_control max_users 2
Command: config mac_based_access_control max_users 2

Success.

DGS-3200-10:4#
```

61-12 config mac_based_access_control authorization attributes

Purpose

To enable or disable the acceptance of an authorized configuration.

Format

config mac_based_access_control authorization attributes {radius [enable | disable] | local [enable | disable]}

Description

This command is used to enable or disable the acceptance of an authorized configuration. When authorization is enabled for MAC-based access controls with RADIUS authentication, the authorized attributes (for example VLAN, 802.1p default priority, and ACL) assigned by the RADUIS server will be accepted if the global authorization status is enabled. When authorization is enabled for MAC-based access controls with local authentication, the authorized attributes assigned by the local database will be accepted.

Parameters

Parameters	Description
radius	Specify to enable or disable the authorized attributes assigned by the RADIUS server that will be accepted.
local	Specify to enable to disable the authorized attributes assigned by the local database.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the configuration authorized from the local database:

```
DGS-3200-10:4# config mac_based_access_control authorization attributes local disable
Command: config mac_based_access_control authorization attributes local disable

Success.

DGS-3200-10:4#
```

61-13 config mac_based_access_control_local

Purpose

To configure the local database entry.

Format

config mac_based_access_control_local mac <macaddr> [vlan <vlan_name 32> | vlanid <1-4094>|clear_vlan]

Description

This command is used to modify a database entry

Parameters

Parameters	Description
mac	The MAC address that access accept by local mode
vlan	If the MAC address is authorized, the port will be assigned to this VLAN.
vlanid	If the MAC address is authorized, the port will be assigned to this VLAN ID.
clear_vlan	Choose to clear the specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure MAC-based access control local:

```
DGS-3200-10::4# config mac_based_access_control_local mac 00-00-00-00-00-01 vlan
default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3200-10:4#
```

61-14 delete mac_based_access_control_local

Purpose

To delete the local database entry.

Format

delete mac_based_access_control_local [mac <macaddr> | vlan <vlan_name 32> | vlanid <1-4094>]

Description

This command is used to delete a database entry

Parameters

Parameters	Description
mac	Delete database by this MAC address.
vlan	Delete database by this VLAN name.
vlanid	Delete database by this VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a MAC-based access control local by MAC address:

```
DGS-3200-10:4# delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DGS-3200-10:4#
```

To delete a MAC-based access control local by VLAN name:

```
DGS-3200-10:4# delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DGS-3200-10:4#
```

61-15 show mac_based_access_control auth_state ports

Purpose

To display MAC-based access control authentication MAC information.

Format

show mac_based_access_control auth_state ports {<portlist>}

Description

This command is used to display MAC-based access control authentication MAC information.

Parameters

Parameters	Description
<portlist>	Specify a list of ports to be displayed

Restrictions

None.

Examples

To display MAC-based access control authentication MAC information:

```
DGS-3200-10:4# show mac_based_access_control auth_state ports
Command: show mac_based_access_control auth_state ports

(P): Port-based   Prio: Priority

Port    MAC Address      Original  State         VID  Prio Aging Time/
                           RX VID                          Block Time
------ -------------------- ---- -------------- ---- ---- -----------
1      00-00-00-00-00-01    1     Authenticated  -    6     1439
1      00-00-12-00-03-00    1     Blocked        -    -     286
3      00-00-00-00-00-02(P) 1     Authenticated  -    6     1440

Total Authenticating Hosts  : 0
Total Authenticated Hosts   : 2
Total Blocked Hosts         : 1

DGS-3200-10:4#
```

61-16 show mac_based_access_control

Purpose

To display the MAC-based access control setting.

Format

show mac_based_access_control {ports {<portlist>}}

Description

This command is used to display the MAC-based access control setting. If no parameter is specified, the Mac-based access control status will be displayed.

Parameters

Parameters	Description
ports	Display the MAC-based access control port state.

Restrictions

None.

Examples

To display MAC-based access control:

```
DGS-3200-10:4#show mac_based_access_control
Command: show mac_based_access_control

MAC-based Access Control
-----------------------------------
State                   : Enabled
Method                  : Local
Password Type           : Manual String
Password                : rosebud
Max User                : No Limit
Guest VLAN              :
Guest VLAN Member Ports:
RADIUS Authorization    : Enabled
Local Authorization     : Enabled
Trap State              : Enabled
Log State               : Enabled

DGS-3200-10:4#
```

To display MAC-based access control for ports 1 to 4:

```
DGS-3200-10:4#show mac_based_access_control port 1-4
Command: show mac_based_access_control ports 1-4



Port    State      Aging Time    Block Time  Max User
                      (min)         (sec)
-----  --------   ----------    ---------   --------
1       Disabled   1440          300          200
2       Disabled   1440          300          200
3       Disabled   1440          300          200
4       Disabled   1440          300          200

DGS-3200-10:4#
```

61-17 show mac_based_access_control_local

Purpose

To display MAC-based access control local databases.

Format

show mac_based_access_control_local {[mac<macaddr>|vlan <vlan_name 32> | vlanid <1-4094>]}

Description

This command is used to display all MAC-based access control local databases.

Parameters

Parameters	Description
mac	Display MAC-based access control local databases by this MAC address.
vlan	Display database by this VLAN name.
vlanid	Display database by this VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display MAC-based access control local:

```
DGS-3200-10:4#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address         VID
-----------------   ----
00-00-00-00-00-01   1
00-00-00-00-00-02   2

Total Entries:2

DGS-3200-10:4#
```

To display MAC-based access control local by MAC address:

```
DGS-3200-10:4#show mac_based_access_control_local mac 00-00-00-00-00-01
Command: show mac_based_access_control_local mac 00-00-00-00-00-01

MAC Address         VID
-----------------   ----
00-00-00-00-00-01   1

Total Entries:1

DGS-3200-10:4#
```

To display MAC-based access control local by VLAN:

```
DGS-3200-10:4#show mac_based_access_control_local vlan default
Command: show mac_based_access_control_local vlan default

MAC Address         VID
-----------------   ----
00-00-00-00-00-01   1

Total Entries:1

DGS-3200-10:4#
```

61-18 config mac_based_access_control log state

Purpose

To enable or disable the generating of MAC-based Access Control logs.

Format

config mac_based_access_control log state [enable | disable]

Description

This command is used to enable or disable the generating of MAC-based Access Control logs.

Parameters

Parameters	Description
enable	Specify to enable the generating of MAC-based Access Control logs.
disable	Specify to disable the generating of MAC-based Access Control logs.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the log state for MAC-based Access Control:

```
DGS-3200-10:4# config mac_based_access_control log state disable
Command: config mac_based_access_control log state disable

Success.

DGS-3200-10:4#
```

61-19 config mac_based_access_control trap state

Purpose

To enable or disable the sending of MAC-based Access Control traps.

Format

config mac_based_access_control trap state [enable | disable]

Description

This command is used to enable or disable the sending of MAC-based Access Control traps.

Parameters

Parameters	Description
enable	Specify to enable the sending of MAC-based Access Control traps.

disable	Specify to disable the sending of MAC-based Access Control traps.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the trap state for MAC-based Access Control:

```
DGS-3200-10:4# config mac_based_access_control trap state enable
Command: config mac_based_access_control trap state enable

Success.

DGS-3200-10:4#
```

61-20 config mac_based_access_control password_type

Purpose

To configure the type of RADIUS authentication password for MAC-based Access Control.

Format

config mac_based_access_control password_type [manual_string | client_mac_address]

Description

This command is used to configure the type of RADIUS authentication password for MAC-based Access Control.

Parameters

Parameters	Description
manual_string	Specify to use the same string as password for all clients do RADIUS authentication, the string can be configured by using the command **config mac_based_access_control password**.
client_mac_address	Specify to use the client's MAC address as the password for RADIUS authentication. The MAC address format can be configured by using the command **config authentication mac_format**.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the MAC-based Access Control using client's MAC address as authentication password:

```
DGS-3200-10:4# config mac_based_access_control password_type client_mac_address
Command: config mac_based_access_control password_type client_mac_address

Success.

DGS-3200-10:4#
```

To configure the MAC-based Access Control using “manual_string” as authentication password:

```
DGS-3200-10:4# config mac_based_access_control password_type manual_string
Command: config mac_based_access_control password_type manual_string

Success.

DGS-3200-10:4#
```

62 JWAC Command List

enable jwac
disable jwac
enable jwac redirect
disable jwac redirect
enable jwac forcible_logout
disable jwac forcible_logout
enable jwac udp_filtering
disable jwac udp_filtering
enable jwac quarantine_server_monitor
disable jwac quarantine_server_monitor
config jwac quarantine_server_error_timeout <sec 5-300>
config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0-10>}
config jwac virtual_ip <ipaddr> {url [<string 128> | clear]}
config jwac quarantine_server_url <string 128>
config jwac clear_quarantine_server_url
config jwac update_server [add | delete] ipaddress <network_address> {[tcp_port <port_number 1-65535> | udp_port <port_number 1-65535>]}
config jwac switch_http_port < tcp_port_number 1-65535> {[http | https]}
config jwac ports [<portlist> | all] {state [enable | disable] | max_authenticating_host <value 0-10> | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}
config jwac radius_protocol [local | pap | chap | ms_chap | ms_chapv2 | eap_md5]
create jwac user <username 15> {vlan <vlanid 1-4094>}
config jwac user <username 15> {vlan <vlanid 1-4094>}
delete jwac [user <username 15> | all_users]
show jwac user
show jwac
show jwac auth_state ports {<portlist>}
show jwac update_server
show jwac ports {<portlist>}
clear jwac auth_state [ports [all | <portlist>] {authenticated | authenticating | blocked} | mac_addr <macaddr>]
config jwac authenticate_page [japanese |english]
config jwac authentication_page element [japanese | english] [default | page_title <desc 128> | login_window_title <desc 32> | user_name_title <desc 16> | password_title <desc 16> | logout_window_title <desc 32> | notification_line <value 1-5> <desc 128>]

show jwac authenticate_page
config jwac authorization attributes {radius [enable | disable] | local [enable | disable]}

62-1 enable jwac

Purpose

To enable the JWAC function.

Format

enable jwac

Description

JWAC and WAC are mutually exclusive functions. That is, they can not be enabled at the same time. Using the JWAC function, PC users need to pass two stages of authentication. The first stage is to do the authentication with the quarantine server and the second stage is the authentication with the switch. For the second stage, the authentication is similar to WAC, except that there is no port VLAN membership change by JWAC after a host passes authentication. The RADIUS server will share the server configuration defined by the 802.1X command set.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To enable JWAC:

```
DGS-3200-10:4# enable jwac
Command: enable jwac

Success.

DGS-3200-10:4#
```

62-2 disable jwac

Purpose

To disable the JWAC function.

Format

disable jwac

Description

This command is used to disable JWAC.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable JWAC:

```
DGS-3200-10:4# disable jwac
Command: disable jwac

Success.

DGS-3200-10:4#
```

62-3 enable jwac redirect

Purpose

To enable the JWAC redirect function.

Format

enable jwac redirect

Description

This command is used to enable JWAC redirect. When **redirect quarantine_server** is enabled, the unauthenticated host will be redirected to a quarantine server when it tries to access a random URL. When **redirect jwac_login_page** is enabled, the unauthenticated host will be redirected to the **jwac_login_page** on the Switch to finish authentication.

Parameters

None.

Restrictions

When enable redirect to quarantine server is in effect, a quarantine server must be configured first. Only Administrator-level users can issue this command.

Example

To enable JWAC redirect:

```
DGS-3200-10:4# enable jwac redirect
Command: enable jwac redirect

Success.

DGS-3200-10:4#
```

62-4 disable jwac redirect

Purpose

To disable the JWAC redirect function.

Format

disable jwac redirect

Description

This command is used to disable JWAC redirect. When redirect is disabled, only access to **quarantine_server** and the **jwac_login_page** from an unauthenticated host is allowed, all other Web access will be denied.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To disable JWAC redirect:

```
DGS-3200-10:4# disable jwac redirect
Command: disable jwac redirect

Success.

DGS-3200-10:4#
```

62-5 enable jwac forcible_logout

Purpose

To enable the JWAC forcible logout function.

Format

enable jwac forcible_logout

Description

This command is used to enable JWAC forcible logout. When enabled, a Ping packet from an authenticated host to the JWAC Switch with TTL=1 will be regarded as a logout request, and the host will be moved back to unauthenticated state.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable JWAC forcible logout:

```
DGS-3200-10:4# enable jwac forcible_logout
Command: enable jwac forcible_logout

Success.

DGS-3200-10:4#
```

62-6 disable jwac forcible_logout

Purpose

To disable the JWAC forcible logout function.

Format

disable jwac forcible_logout

Description

This command is used to disable JWAC forcible logout.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable JWAC forcible logout:

```
DGS-3200-10:4# disable jwac forcible_logout
Command: disable jwac forcible_logout

Success.

DGS-3200-10:4#
```

62-7 enable jwac udp_filtering

Purpose

To enable the JWAC UDP filtering function.

Format

enable jwac udp_filtering

Description

When UDP filtering is enabled, all UDP and ICMP packets except DHCP and DNS packets from unauthenticated hosts will be dropped.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable JWAC UDP filtering:

```
DGS-3200-10:4# enable jwac udp_filtering
Command: enable jwac udp_filtering

Success.

DGS-3200-10:4#
```

62-8 disable jwac udp_filtering

Purpose

To disable the JWAC UDP filtering function.

Format

disable jwac udp_filtering

Description

This command is used to disable JWAC UDP filtering.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable JWAC UDP filtering:

```
DGS-3200-10:4# disable jwac udp_filtering
Command: disable jwac udp_filtering

Success.

DGS-3200-10:4#
```

62-9 enable jwac quarantine_server_monitor

Purpose

To enable the JWAC quarantine server monitor function.

Format

enable jwac quarantine_server_monitor

Description

This command is used to enable the JWAC quarantine server monitor. When enabled, the JWAC switch will monitor the quarantine server to ensure the server is okay. If the switch detects no quarantine server, it will redirect all unauthenticated HTTP accesses to the JWAC Login Page forcibly if the redirect is enabled and the redirect destination is configured to be quarantine server.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable JWAC quarantine server monitoring:

```
DGS-3200-10:4# enable jwac quarantine_server_monitor
Command: enable jwac quarantine_server_monitor

Success.

DGS-3200-10:4#
```

62-10 disable jwac quarantine_server_monitor

Purpose

To disable the JWAC quarantine server monitor function.

Format

disable jwac quarantine_server_monitor

Description

This command is used to disable JWAC quarantine server monitoring.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable JWAC quarantine server monitoring:

```
DGS-3200-10:4# disable jwac quarantine_server_monitor
Command: disable jwac quarantine_server_monitor

Success.

DGS-3200-10:4#
```

62-11 config jwac quarantine_server_error_timeout

Purpose

To set the quarantine server error timeout.

Format

config jwac quarantine_server_error_timeout <sec 5-300>

Description

This command is used to set the quarantine server error timeout. When the quarantine server monitor is enabled, the JWAC switch will periodically check if the quarantine works okay. If the switch does not receive any response from quarantine server during the configured error timeout, the switch then regards it as not working properly.

Parameters

Parameters	Description
<sec 5-300>	Specify the error timeout interval.

Restrictions

Only Administrator-level users can issue this command.

Example

To set the quarantine server error timeout:

```
DGS-3200-10:4# config jwac quarantine_server_error_timeout 60
Command: config jwac quarantine_server_error_timeout 60

Success.

DGS-3200-10:4#
```

62-12 config jwac redirect

Purpose

To configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or JWAC login web page.

Format

config jwac redirect {destination [quarantine_server | jwac_login_page] | delay_time <sec 0-10>}

Description

This command is used to configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or the JWAC login web page. The unit of delay time is seconds.
0 means no delaying the redirect.

Parameters

Parameters	Description
destination	Specify the destination which the unauthenticated host will be redirected to.
delay_time	Specify the time interval after which the unauthenticated host will be redirected.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure redirect destination and delay time before an unauthenticated host is redirected to the quarantine server or JWAC login web page:

```
DGS-3200-10:4# config jwac redirect destination jwac_login_page delay_time 5
Command: config jwac redirect_ destination jwac_login_page delay_time 5

Success.

DGS-3200-10:4#
```

62-13 config jwac virtual_ip

Purpose

To configure JWAC virtual IP addresses used to accept authentication requests from an unauthenticated host.

Format

config jwac virtual_ip <ipaddr>

config jwac virtual_ip <ipaddr> {url [<string 128> | clear]}

Description

The virtual IP of JWAC is used to accept authentication request from unauthenticated host. Only requests sent to this IP will get correct responses. This IP does not respond to ARP requests or ICMP packets.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the virtual IP.
url	This parameter is used to set the URL of virtual IP.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure a JWAC virtual IP address of 1.1.1.1 to accept authentication requests from an unauthenticated host:

```
DGS-3200-10:4# config jwac virtual_ip 1.1.1.1
Command: config jwac virtual_ip 1.1.1.1

Success.

DGS-3200-10:4#
```

62-14 config jwac quarantine_server_url

Purpose

To configure the JWAC quarantine server URL.

Format

config jwac quarantine_server_url <string 128>

Description

This command is used to configure the URL of the quarantine server. If the redirect is enabled and the redirect destination is the quarantine server, when an HTTP request from unauthenticated host not to the quarantine server reaches the JWAC Switch, the Switch will handle this HTTP packet and send back a message to the host or make it access the quarantine server with the configured URL. When the PC connects to the specified URL, the quarantine server will request the PC user to input the user name and password to do authentication.

Parameters

Parameters	Description
<string 128>	Specify the entire URL of the authentication page on the Quarantine Server.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the JWAC quarantine server URL:

```
DGS-3200-10:4# config jwac quarantine_server_url http://10.90.90.88/authpage.html
Command: config jwac quarantine_server_url http://10.90.90.88/authpage.html

Success.

DGS-3200-10:4#
```

62-15 config jwac clear_quarantine_server_url

Purpose

To clear the quarantine server configuration.

Format

config jwac clear_quarantine_server_url

Description

This command is used to clear the quarantine server configuration.

Parameters

None.

Restrictions

When JWAC is enabled and the redirect destination is the quarantine server, the quarantine server cannot be cleared. Only Administrator-level users can issue this command.

Example

To clear the quarantine server configuration:

```
DGS-3200-10:4# config jwac clear_quarantine_server_url
Command: config jwac clear_quarantine_server_url

Success.

DGS-3200-10:4#
```

62-16 config jwac update_server

Purpose

To configure the servers that the PC may need to connect to in order to complete the JWAC authentication.

Format

config jwac update_server [add | delete] ipaddress <network_address>{[tcp_port <port_number 1-65535> | udp_port <port_number 1-65535>]}

Description

This command is used to add or delete a server network address to which the traffic from an unauthenticated client host will not be blocked by the JWAC Switch. Any servers running ActiveX need to be able to have access to accomplish authentication. Before the client passes authentication, it should be added to the Switch with its IP address. For example, the client may need to access update.microsoft.com

or some sites of the Anti-Virus software companies to check whether the OS or Anti-Virus software of the client are the latest; and so IP addresses of update.microsoft.com and of Anti-Virus software companies need to be added in the Switch.

Parameters

Parameters	Description
add	Add a network address to which the traffic will not be blocked. Five network addresses can be added at most.
delete	Delete a network address to which the traffic will not be blocked.
ipaddress	Specify the network address to add or delete.
tcp_port	The accessible TCP port number for the specified update server network.
udp_port	The accessible UDP port number for the specified update server network.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure servers the PC may need to connect to in order to complete JWAC authentication:

```
DGS-3200-10:4# config jwac update_server add ipaddress 10.90.90.109/24
Command: config jwac update_server add ipaddress 10.90.90.109/24

 Update Server 10.90.90.0/24 is added.

Success.

DGS-3200-10:4#
```

62-17 config jwac switch_http_port

Purpose

To configure the TCP port which the JWAC switch listens to.

Format

config jwac switch_http_port < tcp_port_number 1-65535> {[http | https]}

Description

This command is used to configure the TCP port which the JWAC switch listens to. This port number is used in the second stage of the authentication. PC users will connect to the page on the switch to input the user name and password. If not specified, the default port number is 80. If no protocol is specified, the protocol is HTTP.

Parameters

Parameters	Description
<tcp_port_number 1-65535>	A TCP port which the JWAC Switch listens to and uses to finish the authenticating process.
http	Specify the JWAC run HTTP protocol on this TCP port.
https	Specify the JWAC run HTTPS protocol on this TCP port.

Restrictions

HTTP cannot run on TCP port 443, and HTTPS cannot run on TCP port 80. Only Administrator-level users can issue this command.

Example

To configure the TCP port which the JWAC switch listens to:

```
DGS-3200-10:4# config jwac switch_http_port 8888 http
Command: config jwac switch_http_port 8888 http

Success.

DGS-3200-10:4#
```

62-18 config jwac ports

Purpose

To configure the port state of JWAC.

Format

config jwac ports [<portlist> | all] {state [enable | disable] | max_authenticating_host <value 0-10> | aging_time [infinite | <min 1-1440>] | idle_time [infinite | <min 1-1440>] | block_time [<sec 0-300>]}

Description

This command is used to configure port state of JWAC. The default value of the **max_authenticating_host** is 10. The default value of the **aging_time** is 1440 minutes. The default value of the **idle_time** is infinite. The default value of the **block_time** is 0 seconds.

Parameters

Parameters	Description
<porlist>	A port range for setting the JWAC state.
all	Every Switch ports' JWAC state is configured.
state	Specify the port state of JWAC.
max_authenticating_host	The maximum number of hosts that can process authentication

	on each port at the same time.
aging_time	A time period during which an authenticated host will keep in authenticated state. **infinite** indicates never aging out the authenticated host on the port.
idle_time	If there is no traffic during idle time, the host will be moved back to unauthenticated state. **infinite** indicates never checking the idle state of the authenticated host on the port.
block_time	If a host fail to pass the authentication, it will be blocked for a period specified by the block time.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the JWAC port state:

```
DGS-3200-10:4# config jwac port 1-9 state enable
Command: config jwac port 1-9 state enable

Success.

DGS-3200-10:4#
```

62-19 config jwac radius_protocol

Purpose

To configure the RADIUS protocol used by JWAC.

Format

config jwac radius_protocol [local | pap | chap | ms_chap | ms_chapv2 | eap_md5]

Description

This command is used to specify the RADIUS protocol used by JWAC to complete RADIUS authentication.

Parameters

Parameters	Description
local	JWAC Switch uses local user DB to complete the authentication.
pap	JWAC Switch uses PAP to communicate with the RADIUS Server.
chap	JWAC Switch uses CHAP to communicate with the RADIUS Server.
ms_chap	JWAC Switch uses MS-CHAP to communicate with the RADIUS Server.

ms_chapv2	JWAC Switch uses MS-CHAPv2 to communicate with the RADIUS Server.
eap_md5	JWAC Switch uses EAP MD5 to communicate with the RADIUS Server.

Restrictions

JWAC shares other RADIUS configurations with 802.1x. When using this command to set the RADIUS protocol, you must make sure the RADIUS server added by the **config radius** command supports the protocol. Only Administrator-level users can issue this command.

Example

To configure the RADIUS protocol used by JWAC:

```
DGS-3200-10:4# config jwac radius_protocol ms_chapv2
Command: config jwac radius_protocol ms_chapv2

Success.

DGS-3200-10:4#
```

62-20 create jwac user

Purpose

To create a JWAC user in the local DB.

Format

create jwac user <username 15> {vlan <vlanid 1-4094>}

config jwac user <username 15> {vlan <vlanid 1-4094>}

Description

This command creates JWAC users in the local DB. When “local” is chosen while configuring the JWAC RADIUS protocol, the local DB will be used.

Parameters

Parameters	Description
<username 15>	The user name to be created.
<vlanid 1-4094>	Target VLAN ID for authenticated host which uses this user account to pass authentication.

Restrictions

Only Administrator-level users can issue this command.

Example

To create a JWAC user in the local DB:

```
DGS-3200-10:4# create jwac user 112233
Command: create jwac user 112233

Enter a case-sensitive new password:***
Enter the new password again for confirmation:***
Success.

DGS-3200-10:4#
```

62-21 delete jwac user

Purpose

To delete a JWAC user into the local DB.

Format

delete jwac [user <username 15> | all_users]

Description

This command is used to delete JWAC users from the local DB.

Parameters

Parameters	Description
user	Specify the user name to be deleted
all_users	All user accounts in local DB will be deleted.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a JWAC user from the local DB:

```
DGS-3200-10:4# delete jwac user 112233
Command: delete jwac user 112233

Success.

DGS-3200-10:4#
```

62-22 show jwac user

Purpose

To display a JWAC user in the local DB.

Format

show jwac user

Description

This command is used to display JWAC users in the local DB.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the current JWAC users in the local DB:

```
DGS-3200-10:4# show jwac user
Command: show jwac user

User Name          Password           VID
---------------   ----------------   ----------
admin              test               -



Total Entries:1

DGS-3200-10:4#
```

62-23 show jwac

Purpose

To display the JWAC configuration.

Format

show jwac

Description

This command is used to display the JWAC configuration settings.

Parameters

None.

Restrictions

None.

Example

To display the current JWAC configuration:

```
 DGS-3200-10:4# show jwac
 Command: show jwac

State                    : Enabled
Enabled Ports            : 1:1,1:11,1:23,1:25,1:35
Virtual IP/URL           : 1.1.1.1/www.kyoto.ac.jp
Switch HTTP Port         : 21212 (HTTP)
UDP Filtering            : Enabled
Forcible Logout          : Enabled
Redirect State           : Enabled
Redirect Delay Time      : 3 Seconds
Redirect Destination     : Quarantine Server
Quarantine Server        : http://172.18.212.147/pcinventory
Q-Server Monitor         : Enabled (Running)
Q-Server Error Timeout   : 5 Seconds
RADIUS Auth-Protocol     : PAP
RADIUS Authorization     : Enabled
Local Authorization      : Enabled

 DGS-3200-10:4#
```

62-24 show jwac auth_state ports

Purpose

To display information for JWAC client hosts.

Format

show jwac auth_state ports {<portlist>}

Description

This command is used to display information for JWAC client hosts.

Parameters

Parameters	Description
<portlist>	Specify a port range to show the JWAC authentication entries. If no port is specified, the JWAC authentication state will be displayed for all ports.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display JWAC authentication entries for ports 1 to 2:

```
DGS-3200-10:4# show jwac auth_state ports 1-3
Command: show jwac auth_state ports 1-3
Pri - Priority. State - A:Authenticated, B:Blocked, -:Authenticating
Time - Aging Time/Idle Time for authenticated entries.

Port  MAC Address        State VID Pri  Time            IP              User Name
----- -----------------   -- ---- -- -------- ---------------- ----------------
1     00-00-00-00-00-01    A 20   3  -/40     192.168.101.239  juser_tom
1     00-00-00-00-00-02    A 1234 -  -/50     172.18.61.242    name_of_15chars
1     00-00-00-00-00-03    B -    -  60       172.18.61.242    Jack
1     00-00-00-00-00-04    - -    -  10        -                -
2     00-00-00-00-00-10(P) A 1234 2  1440/20  10.10.10.90      jane
3     00-00-00-00-00-20(P) - -    -  20        10.10.10.131     -
3     00-00-00-00-00-21(P) B -    -  200      -                Victor
Total Authenticating Hosts   : 2
Total Authenticated Hosts    : 3
Total Blocked Hosts          : 2

DGS-3200-10:4#
```

62-25 show jwac update_server

Purpose

To display the JWAC update server.

Format

show jwac update_server

Description

This command is used to display the JWAC update server.

Parameters

None.

Restrictions

None.

Examples

To display the JWAC update server:

```
DGS-3200-10:4# show jwac update_server
Command: show jwac update_server

Index  IP                      TCP/UDP  Port   State
-----  ------------------  -------  -----  --------
1      10.0.0.0/8          -        -      Inactive
2      10.1.1.1/32         UDP      90     Inactive
3      10.3.3.3/32         TCP      80     Inactive
4      10.3.3.4/32         -        -      Inactive
5      10.3.3.5/32         -        -      Inactive
6      10.3.3.6/32         -        -      Inactive
7      10.3.3.7/32         -        -      Inactive
8      10.3.3.9/32         -        -      Inactive
9      10.3.3.10/32        -        -      Inactive
10     100.100.100.100/32  TCP      9080   Inactive

DGS-3200-10:4#
```

62-26 show jwac ports

Purpose

To display the port configuration of JWAC.

Format

show jwac ports {<portlist>}

Description

This command is used to display the port configuration of JWAC.

Parameters

Parameters	Description
<portlist>	Specify a port range to show the configuration of JWAC.

Restrictions

None.

Example

To display JWAC ports 1 to 4:

```
DGS-3200-10:4# show jwac port 1-4
Command: show jwac port 1-4

Port   State     Aging Time  Idle Time  Block Time  Max
                     (min)      (min)      (sec)     Hosts
 -----  --------  ----------  ---------  ----------  -----
 1      Enabled   Infinite    200        10          10
 2      Disabled  600         30         60          10
 3      Disabled  1440        Infinite   60          10
 4      Disabled  1000        Infinite   30          10

DGS-3200-10:4#
```

62-27 clear jwac auth_state

Purpose

To delete the authentication entries.

Format

clear jwac auth_state [ports [all | <portlist>] {authenticated | authenticating | blocked} | mac_addr <macaddr>]

Description

This command is used to clear authentication entries.

Parameters

Parameters	Description
ports	Specify the range of ports on which the authentication entries will be deleted.
authenticated	Specify to delete the authenticated entries on port(s) specified by parameter ports.
authenticating	Specify to delete the authenticating entries on port(s) specified by parameter ports.
blocked	Specify to delete the blocked entries on port(s) specified by parameter ports.
<macaddr>	Specify to delete the special entries identified by MAC address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete authentication entries:

```
DGS-3200-10:4#clear jwac auth_state ports all blocked
Command: clear jwac auth_state ports all blocked

Success.

DGS-3200-10:4#
```

62-28 config jwac authenticate_page

Purpose

To customize the authenticate page.

Format

config jwac authenticate_page [japanese |english]

Description

This command is used to customize the JWAC authenticate page.

Parameters

Parameters	Description
japanese	Change to Japanese page.
english	Change to English page.

Restrictions

Only Administrator-level users can issue this command.

Example

To customize the authenticate page:

```
DGS-3200-10:4#config jwac authenticate_page japanese
Command: config jwac authenticate_page japanese

Success.

DGS-3200-10:4#
```

62-29 config jwac authentication_page element

Purpose

To customize the JWAC authenticate page.

Format

config jwac authentication_page element [japanese | english] [default | page_title <desc 128> | login_window_title <desc 32> | user_name_title <desc 16> | password_title <desc 16> | logout_window_title <desc 32> | notification_line <value 1-5> <desc 128>]

Description

This command is used to customize the JWAC authenticate page by administrators.

Parameters

Parameters	Description
japanese	Specify to change to the Japanese page.
english	Specify to change to the English page.
default	Specify to reset the page element to default.
page_title	Specify the title of the authenticate page.
login_window_title	Specify the login window title of the authenticate page.
user_name_title	Specify the user name title of the authenticate page.
password_title	Specify the password title of the authenticate page.
logout_window_title	Specify the logout windown title mapping of the authenticate page.
notification_line	Specify this parameter to set the notification information by line in authentication Web pages.

Restrictions

Only Administrator-level users can issue this command.

Examples

To customize the authenticate page:

```
DGS-3200-10:4# config jwac authentication_page element japanese page_title "ディーリンクジャパン株式会社
"
Command: config jwac authentication_page element japanese page_title "ディーリンクジャパン株式会社"

Success.

DGS-3200-10:4#
```

62-30 show jwac authenticate_page

Purpose

To display the element mapping of the customized authenticate page.

Format

show jwac authenticate_page

Description

This command is used to display the element mapping of the customized authenticate page.

Parameters

None.

Restrictions

None.

Examples

To display the element mapping of the customized authenticate page:

```
DGS-3200-10:4#show jwac authenticate_page
Command: show jwac authenticate_page

 Current Page : English Version
English Page Element
------------------------------------------------------------
Page Title           :
Login Window Title    : Authentication Login
User Name Title      : User Name
Password Title       : Password
Logout Window Title   : Logout from the network
Notification        :



Japanese Page Element
------------------------------------------------------------
Page Title           :
Login Window Title    : 社内 LAN 認証ログイン
User Name Title       : ユーザ ID
Password Title        : パスワード
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

62-31 config jwac authorization attributes

Purpose

To enable acceptation of authorized configuration.

Format

config jwac authorization attributes {radius [enable | disable] | local [enable | disable]}

Description

This command is used to enable or disable acceptation of authorized configuration. When the authorization is enabled for JWAC's RADIUS, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled. When the authorization is enabled for JWAC's local, the authorized data assigned by the local database will be accepted.

Parameters

Parameters	Description
radius	Specify to enable or disable authorized data assigned by the RADUIS server to be accepted. If specified to enable, the authorized data assigned by the RADUIS server will be accepted if the global authorization network is enabled.The default state is enabled.
local	Specify to enable or disable authorized data assigned by the local database to be accepted. If specified to enable, the authorized data assigned by the local database will be accepted if the global authorization network is enabled. The default state is enabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the configuration authorized from the local database:

```
DGS-3200-10:4# config jwac authorization attributes local disable
Command: config jwac authorization attributes local disable

Success.

DGS-3200-10:4#
```

63 Compound Authentication Command List

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]
config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add|delete] ports [<portlist> | all]
config authentication mac_format {case [lowercase | uppercase] | delimiter{[hyphen | colon | dot | none] | number [1 | 2 | 5]}}
config authentication ports [<portlist> | all] {auth_mode [port_based | host_based] | multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac | mac_impb]}
show authentication guest_vlan
show authentication ports {<portlist>}
enable authorization attributes
disable authorization attributes
show authorization
config authentication server failover [local | permit | block]
show authentication
show authentication mac_format

63-1 create authentication guest_vlan

Purpose

To assign a static VLAN to be a guest VLAN.

Format

create authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Description

This command is used to assign a static VLAN to be a guest VLAN. The specific VLAN which is assigned to be a guest VLAN must already exist. The specific VLAN which is assigned to be a guest VLAN can't be deleted.

For further description of this command, please see the description for **config authentication guest_vlan ports**.

Parameters

Parameters	Description
vlan_name 32	Specify the guest VLAN by VLAN name.
vlanid	Specify the guest VLAN by VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Example

To assign a static VLAN to be a guest VLAN:

```
DGS-3200-10:4# create authentication guest_vlan vlan guestVLAN
Command: create authentication guest_vlan vlan guestVLAN

Success.

DGS-3200-10:4#
```

63-2 delete authentication guest_vlan

Purpose

To delete a guest VLAN configuration.

Format

delete authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>]

Description

This command is used to delete a guest VLAN setting, but not a static VLAN. All ports which are enabled as guest VLANs will move to the original VLAN after deleting the guest VLAN. For further description of this command, please see the description for **config authentication guest_vlan ports**.

Parameters

Parameters	Description
vlan_name 32	Specify the guest VLAN by VLAN name.
vlanid	Specify the guest VLAN by VLAN ID.

Restrictions

Only Administrator-level users can issue this command.

Example

To delete a guest VLAN setting:

```
DGS-3200-10:4# delete authentication guest_vlan vlan guestVLAN
Command: delete authentication guest_vlan vlan guestVLAN

Success.

DGS-3200-10:4#
```

63-3 config authentication guest_vlan ports

Purpose

To configure security port(s) as specified guest VLAN members.

Format

config authentication guest_vlan [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] [add | delete] ports [<portlist> |all]

Description

This command is used to assign or remove ports to or from a guest VLAN.

Parameters

Parameters	Description
vlan_name	Assign a VLAN as a guest VLAN. The VLAN must be an existing static VLAN.
vlanid	Assign a VLAN as a guest VLAN. The VLAN must be an existing static VLAN.
add	Specify to add a port list to the guest VLAN.
delete	Specify to delete a port list from the guest VLAN.
portlist	Specify the configured port(s).

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure authentication for all ports for a guest VLAN called “gv”:

```
DGS-3200-10:4# config authentication guest_vlan vlan gv add ports all
Command: config authentication guest_vlan vlan gv add ports all

Success.

DGS-3200-10:4#
```

63-4 config authentication mac_format

Purpose

To configure the MAC address format used for authentication username via the RADIUS server.

Format

config authentication mac_format {case [lowercase | uppercase] | delimiter{[hyphen | colon | dot |

none] | number [1 | 2 | 5]}}

Description

This command is used to configure the MAC address format used for authentication username via the RADIUS server.

Parameters

Parameters	Description
case	**lowercase** - Using lowercase format, the RADIUS authentication username will be formatted as: aa-bb-cc-dd-ee-ff. **uppercase** - Using uppercase format, the RADIUS authentication username will be formatted as: AA-BB-CC-DD-EE-FF.
delimiter	**hyphen** - Using "-" as delimiter, the format is: AA-BB-CC-DD-EE-FF. **colon** - Using ":" as delimiter, the format is: AA:BB:CC:DD:EE:FF. **dot** - Using "." as delimiter, the format is: AA.BB.CC.DD.EE.FF. **non** - Not using any delimiter, the format is: AABBCCDDEEFF.
number	Specifies the delimiter number used. **1** - Single delimiter, the format is: AABBCC.DDEEFF. **2** - Double delimiter, the format is: AABB.CCDD.EEFF. **5** - Multiple delimiter, the format is: AA.BB.CC.DD.EE.FF.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the MAC address format to IETF style:

```
DGS-3200-10:4#config authentication mac_format case uppercase delimiter hyphen number
5
Command: config authentication mac_format case uppercase delimiter hyphen number 5

Success.

DGS-3200-10:4#
```

63-5 config authentication ports

Purpose

To configure security port(s).

Format

config authentication ports [<portlist> | all] {auth_mode [port_based | host_based] |

multi_authen_methods [none | any | dot1x_impb | impb_jwac | impb_wac | mac_impb]}

Description

This command is used to configure authorization mode and authentication method on ports.

Parameters

Parameters	Description
portlist	Port(s) to configure.
auth_mode	**port-based**: If one of the attached hosts pass the authentication, all hosts on the same port will be granted access to the network. If the user fails the authorization, this port will keep trying the next authentication **host-based**: Every user can be authenticated individually.
multi_authen_methods	Specify the method for multiple authentication.
none	Multiple authentication is not enabled.
any	If any one of the authentication methods (802.1x, MAC, and JWAC/WAC) passes, then pass.
dot1x_impb	802.1X will be verified first, and then IMPB will be verified. Both authentications need to be passed.
impb_jwac	JWAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.
impb_wac	WAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.
mac_impb	MAC will be verified first, and then IMPB will be verified. Both authentications need to be passed.

Restrictions

Only Administrator-level users can issue this command.

Examples

The following example sets the authentication mode of all ports to host-based:

```
DGS-3200-10:4# config authentication ports all auth_mode host_based
Command: config authentication ports all auth_mode host_based

Success.

DGS-3200-10:4#
```

The following example sets the multi-authentication method of all ports to “any”:

```
DGS-3200-10:4# config authentication ports all multi_authen_methods any
Command: config authentication ports all multi_authen_methods any

Success.

DGS-3200-10:4#
```

63-6 show authentication guest_vlan

Purpose

To display the guest VLAN setting.

Format

show authentication guest_vlan

Description

This command is used to display guest VLAN information.

Parameters

None.

Restrictions

None.

Examples

To display the guest VLAN setting:

```
DGS-3200-10:4#show authentication guest_vlan
Command: show authentication guest_vlan

Guest VLAN VID          :
Guest VLAN Member Ports:

 Total Entries: 0



DGS-3200-10:4#
```

63-7 show authentication ports

Purpose

To display the authentication setting on port(s).

Format

show authentication ports {<portlist>}

Description

This command is used to display the authentication method and authorization mode on ports.

Parameters

Parameters	Description
portlist	Display multiple authentication on specific port(s).

Restrictions

None.

Example

To display the authentication settings for all ports:

```
DGS-3200-10:4#show authentication ports
Command: show authentication ports

 Port  Methods         Auth Mode
 ---- -------------- -----------
 1    None           Host_based
 2    Any            Host_based
 3    802.1X_IMPB    Host_based
 4    None           Host_based
 5    None           Host_based
 6    IMPB_JWAC      Host_based
 7    None           Host_based
 8    None           Host_based
 9    802.1X_IMPB    Host_based
 10   None           Host_based

DGS-3200-10:4#
```

63-8 enable authorization attributes

Purpose

To enable the authorization global state.

Format

enable authorization attributes

Description

This command is used to enable the authorization global state. When the authorization for attributes are enabled, whether the authorized attributes (for example, VLAN, 802.1p default priority and ACL) assigned by the RADUIS server or local database will be accepted depending on the individual module's settings. Authorization for attributes is enabled by default.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the authorization global state:

```
DGS-3200-10:4# enable authorization attributes
Command: enable authorization attributes

Success.

DGS-3200-10:4#
```

63-9 disable authorization attributes

Purpose

To disable the authorization global state.

Format

disable authorization attributes

Description

This command is used to disable the authorization global state. When the authorization for attributes are disabled, the authorized attributes (for example, VLAN, 802.1p default priority and ACL) assigned by the RADUIS server or local database will be ignored even if the individual module's setting is enabled. Authorization for attributes is enabled by default.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the authorization global state:

```
DGS-3200-10:4# disable authorization attributes
Command: disable authorization attributes

Success.

DGS-3200-10:4#
```

63-10 show authorization

Purpose

To display the authorization status.

Format

show authorization

Description

This command is used to display the authorization status.

Parameters

None.

Restrictions

None.

Example

To display the authorization status:

```
DGS-3200-10:4#show authorization
Command: show authorization

Authorization for Attributes: Enabled

DGS-3200-10:4#
```

63-11 config authentication server failover

Purpose

To configure the authentication server failover function.

Format

config authentication server failover [local | permit | block]

Description

This command is used to configure the authentication server failover function. When authentication server fails, administrator can configure to:

- Use the local database to authenticate the client. The switch will resort to using the local database to authenticate the client. If the client fails on local authentication, the client is regarded as un-authenticated, otherwise, it authenticated.
- Pass authentication. The client is always regarded as authenticated. If guest VLAN is enabled, clients will stay on the guest VLAN, otherwise, they will stay on the original VLAN.
- Block the client (default setting). The client is always regarded as un-authenticated.

Parameters

Parameters	Description
local	Specify to use the local database to authenticate the client.
permit	Specify that the client is always regarded as authenticated.
block	Specify to block the client. This is the default setting.

Restrictions

Only Administrator-level users can issue this command.

Examples

To set the authentication server failover state:

```
DGS-3200-10:4#config authentication server failover local
Command: config authentication server failover local

Success.

DGS-3200-10:4#
```

63-12 show authentication

Purpose

To display the global authentication configuration.

Format

show authentication

Description

This command is used to display the global authentication configuration.

Parameters

None.

Restrictions

None.

Examples

To display the global authentication configuration:

```
DGS-3200-10:4# show authentication
Command: show authentication

Authentication Server Failover: Block.

DGS-3200-10:4#
```

63-13 show authentication mac_format

Purpose

To display the authentication MAC format setting.

Format

show authentication mac_format

Description

This command is used to display the authentication MAC format setting.

Parameters

None.

Restrictions

None.

Examples

To display the authentication MAC format setting:

```
DGS-3200-10:4# show authentication mac_format
Command: show authentication mac_format

 Case               : Uppercase
 Delimiter          : None
 Delimiter Number   : 5

DGS-3200-10:4#
```

64 Filter Command List

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all]|ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]
show filter dhcp_server

64-1 config filter dhcp_server

Purpose

To configure the state of the function for filtering of DHCP server packets and to add or delete the DHCP server or client binding entry.

Format

config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all] | delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist> | all]|ports [<portlist> | all] state [enable | disable] | illegal_server_log_suppress_duration [1min | 5min | 30min] | trap_log [enable | disable]]

Description

This command has two purposes: to specify to filter all DHCP server packets on the specific port and to specify to allow some DHCP server packets with pre-defined server IP addresses and client MAC addresses. With this function, we can restrict the DHCP server to service specific DHCP clients. This is useful when two DHCP servers are present on the network; one of them can provide the private IP address and the other can provide the public IP address.

Enabling filter DHCP server port state will create one access profile and create one access rule per port (UDP port = 68). Filter commands in this file will share the same access profile.

Addition of a permit DHCP entry will create one access profile and create one access rule. Filter commands in this file will share the same access profile.

Parameters

Parameters	Description
<ipaddr>	The IP address of the DHCP server to be filtered.
<macaddr>	The MAC address of the DHCP client.
ports	The port number of filter DHCP server.
state	Enable or disable the filter DHCP server state
illegal_server_log_suppress_duration	The same illegal DHCP server IP address detected

	will be logged only once within the duration. The log can be suppressed by one minute, 5 minutes, or 30 minutes. The default value is 5 minutes.
trap_log	Enable or disable traps or logs related to DHCP server filter.

Restrictions

Only Administrator-level users can issue this command.

Example

To add an entry from the DHCP server/client filter list in the Switch's database:

```
DGS-3200-10:4# config filter dhcp_server add permit server ip 10.1.1.1 client_mac
00-00-00-00-00-01 ports 1-10
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac
00-00-00-00-00-01 ports 1-10

Success.

DGS-3200-10:4#
```

To configure the filter DHCP server state:

```
DGS-3200-10:4# config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success.

DGS-3200-10:4#
```

64-2 show filter dhcp_server

Purpose

To display the DHCP server/client filter list created on the Switch.

Format

show filter dhcp_server

Description

This command is used to display the DHCP server/client filter list created on the Switch.

Parameters

None.

Restrictions

None.

Example

To display the DHCP server/client filter list created on the switch:

```
DGS-3200-10:4#show filter dhcp_server
Command: show filter dhcp_server
Filter DHCP Server Trap_Log State        : Disabled
Enabled Ports                            :
Illegal Server Log Suppress Duration    : 5 minutes

Filter DHCP Server/Client Table
Server IP Address   Client MAC address   Port
-----------------  -------------------  ---------------
Total Entries:  0

DGS-3200-10:4#
```

65 ARP Spoofing Prevention Command List

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist>|all] | delete gateway_ip <ipaddr>]
show arp_spoofing_prevention

65-1 config arp_spoofing_prevention

Purpose

To configure the prevention of ARP spoofing attacks.

Format

config arp_spoofing_prevention [add gateway_ip <ipaddr> gateway_mac <macaddr> ports [<portlist>|all] | delete gateway_ip <ipaddr>]

Description

This command is used to configure the prevention of ARP spoofing attacks.

Parameters

Parameters	Description		
add	**gateway_ip**	Specify a gateway IP to be configured.	
	gateway_mac	Specify a gateway MAC to be configured.	
	ports	**portlist**	Specify a range of ports to be configured.
		all	Specify all ports to be configured.
delete	**gateway_ip**	Specify a gateway IP to be configured.	

Restrictions

Only Administrator-level users can issue this command.

Example

To configure the prevention of ARP spoofing attacks:

```
 DGS-3200-10:4#config arp_spoofing_prevention add gateway_ip 10.254.254.254
gateway_mac 00-00-00-11-11-11 ports 1-2
 Command: config arp_spoofing_prevention add gateway_ip 10.254.254.254 gateway_mac
00-00-00-11-11-11 ports 1-2

 Success.

 DGS-3200-10:4#
```

65-2 show arp_spoofing_prevention

Purpose

To display the ARP spoofing prevention entry.

Format

show arp_spoofing_prevention

Description

This command is used to display the ARP spoofing prevention entry.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Example

To display the ARP spoofing prevention entry:

```
DGS-3200-10:4#show arp_spoofing_prevention
Command: show arp_spoofing_prevention

ARP Spoofing Prevention Table
Gateway IP Address Gateway MAC Address  Port
------------------ --------------------  ----------------------
10.254.254.254     00-00-00-11-11-11     1-2

 Total Entries: 1

DGS-3200-10:4#
```

66 CPU Filter Command List

config cpu_filter l3_control_pkt <portlist> [{dvmrp | pim | igmp_query |ospf | rip | vrrp} | all] state [enable | disable]
show cpu_filter l3_control_pkt ports {<portlist>}

66-1 config cpu_filter l3_control_pkt

Purpose

To discard Layer 3 control packets sent to the CPU from specific ports.

Format

config cpu_filter l3_control_pkt <portlist> [{dvmrp | pim | igmp_query |ospf | rip | vrrp} | all] state [enable | disable]

Description

This command is used to discard Layer 3 control packets sent to the CPU from specific ports.

Parameters

Parameters	Description
portlist	Specify the port list to filter control packets.
dvmrp **pim** **igmp_query** **ospf** **rip** **vrrp**	The protocols to filter. Specify all to filter all the Layer 3 control packets.
state	Enable or disable the filtering function. The default is disabled.

Restrictions

Only Administrator-level users can issue this command.

Example

To filter DVMRP and OSPF on ports 1 to 10:

```
DGS-3200-10:4#config cpu_filter l3_control_pkt 2-5 all state enable
Command: config cpu_filter l3_control_pkt 2-5 all state enable

Success.

DGS-3200-10:4#
```

66-2 show cpu_filter l3_control_pkt ports

Purpose

To display Layer 3 control packets sent to the CPU from specific ports.

Format

show cpu_filter l3_control_pkt ports {<portlist>}

Description

This command is used to display Layer 3 control packets sent to the CPU from specific ports.

Parameters

Parameters	Description
<portlist>	Specify a list of ports to be displayed.

Restrictions

None.

Examples

To display Layer 3 control packets sent to the CPU from all ports:

```
DGS-3200-10:4#show cpu_filter l3_control_pkt ports
Command: show cpu_filter l3_control_pkt ports

 Port   IGMP-Query    DVMRP     PIM       OSPF       RIP       VRRP
 ----   ----------   -------   -------   -------   -------   -------
 1      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 2      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 3      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 4      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 5      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 6      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 7      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 8      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 9      Disabled     Disabled  Disabled  Disabled  Disabled  Disabled
 10     Disabled     Disabled  Disabled  Disabled  Disabled  Disabled

DGS-3200-10:4#
```

IX. QoS

The QoS section includes the following chapter: QoS.

67 QoS Command List

config bandwidth_control [<portlist>|all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit | <value 64-1024000>]}
show bandwidth_control {<portlist>}
config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {max_rate [no_limit | <value 64-1024000>]}
show per_queue bandwidth_control {<portlist>}
config scheduling <class_id 0-7> max_packet<value 0-255>
config scheduling_mechanism [strict | weight_fair]
show scheduling
show scheduling_mechanism
config 802.1p user_priority <priority 0-7> <class_id 0-7>
show 802.1p user_priority
config 802.1p default_priority [<portlist> | all] <priority 0-7>
show 802.1p default_priority { <portlist>}

67-1 config bandwidth_control

Purpose

To configure the port bandwidth limit control.

Format

config bandwidth_control [<portlist>|all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit |<value 64-1024000>]}

Description

This command is used to set the maximum limit for port bandwidth.

Parameters

Parameters	Description
portlist	Specify a range of ports to be configured.
rx_rate	Specify the limitation of receive data rate.

	no_limit - Indicates there is no limit on port rx bandwidth. An integer value from 64 to 1024000 sets a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. This exact logical limit or token value is hardware determined. The token value will always be a multiple of the bandwidth increment specific to the chip used for the project (i.e. 32 Kbits, 64 Kbits, 128 Kbits, etc.). This token value, the actual set limit recognized by the CPU, will be displayed when the user enters the bandwidth limit integer. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits.
tx_rate	Specifies the limitation of transmit data rate.
	no_limit - Indicates there is no limit on port tx bandwidth. An integer value from 64 to 1024000 sets a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. This exact logical limit or token value is hardware determined. The token value will always be a multiple of the bandwidth increment specific to the chip used for the project (i.e. 32 Kbits, 64 Kbits, 128 Kbits, etc.). This token value, the actual set limit recognized by the CPU, will be displayed when the user enters the bandwidth limit integer. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port bandwidth:

```
DGS-3200-10:4#config bandwidth_control 1-10 tx_rate 1024
Command: config bandwidth_control 1-10 tx_rate 1024

Success.

DGS-3200-10:4#
```

Response messages

(1). "**Success.**"

When users input a value that is a multiple of 64 and the setting is successful.

(2). "**Fail !**

Trunk member port can not be configured because the master is not contained in the portlist" .

The configured portlist contains trunk port but not it's master port.

67-2 show bandwidth_control

Purpose

To display the port bandwidth control table.

Format

show bandwidth_control {<portlist>}

Description

This command is used to display the port bandwidth configurations. If no parameter is specified, the system will display all port bandwidth configurations.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display the port bandwidth control table:

```
DGS-3200-10:4#show bandwidth_control  1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port   RX Rate        TX Rate       Effective RX         Effective TX
       (Kbit/sec)     (Kbit/sec)     (Kbit/sec)           (Kbit/sec)
----   ----------     ----------     ----------------     ----------------
 1     no_limit       no_limit       no_limit             no_limit
 2     no_limit       no_limit       no_limit             no_limit
 3     no_limit       no_limit       no_limit             no_limit
 4     no_limit       no_limit       no_limit             no_limit
 5     no_limit       no_limit       no_limit             no_limit
 6     no_limit       no_limit       no_limit             no_limit
 7     no_limit       no_limit       no_limit             no_limit
 8     no_limit       no_limit       no_limit             no_limit
 9     no_limit       no_limit       no_limit             no_limit
 10   no_limit     no_limit     no_limit          no_limit

DGS-3200-10:4#
```

67-3 config per_queue bandwidth_control

Purpose

To set the bandwidth control for each specific egress queue on specified ports.

Format

config per_queue bandwidth_control {ports [<portlist> | all]} <cos_id_list 0-7> {max_rate [no_limit | <value 64-1024000>]}

Description

This command is used to set the bandwidth control for each specific egress queue on specified ports. The maximum rate limits the bandwidth. When specified, packets transmitted from the queue will not exceed the specified limit even if extra bandwidth is available. The specification of maximum rate is effective regardless of whether the queue is operating in strict or Shaped Deficit Weighted Round Robin (SDWRR) mode.

Parameters

Parameters	Description
ports	Specify a range of ports or all ports to be configured.
<cos_id_list 0-7>	Specify a list of priority queues. The priority queue number ranges from 0 to 7.
max_rate	Specify one of the parameters below will be applied to the maximum rate that the class specified above will be allowed to transmit packets at. **no_limit** - Indicate there is no limit on egress queue of specified port bandwidth. **<value 64-1024000>** - Specify an integer value from 64 to 10240000 to set a maximum limit in Kbits/sec. The specified bandwidth limit may be equaled but not exceeded. The exact logical limit or token value is hardware determined. Note: 1 Kbit = 1000 bits, 1 Gigabit = 1000*1000 Kbits. Actual rate = (inputted rate/ 64) * 64.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the maximum rate to be 100 on queue 1 for ports 1 to 5:

```
DGS-3200-10:4# config per_queue bandwidth_control ports 1-5 1 max_rate 100
Command: config per_queue bandwidth_control ports 1-5 1 max_rate 100

 Granularity: TX: 64. Actual Rate: MAX: 64.

Success.

DGS-3200-10:4#
```

67-4 show per_queue bandwidth_control

Purpose

To display the bandwidth control setting of per egress queue for each port.

Format

show per_queue bandwidth_control {<portlist>}

Description

This command is used to display the bandwidth control setting of per egress queue for each port.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display the port bandwidth control table for port 1:

```
DGS-3200-10:4# show per_queue bandwidth_control 1
Command: show per_queue bandwidth_control 1

Queue Bandwidth Control Table On Port: 1

Queue      Max Rate(Kbit/sec)
0          No Limit
1          64
2          No Limit
3          No Limit
4          No Limit
5          No Limit
6          No Limit
7          No Limit

DGS-3200-10:4#
```

67-5 config scheduling

Purpose

To configure the packets proportion of the appointed class for the weight_fair mechanism.

Format

config scheduling <class_id 0-7> max_packet <value 0-255>

Description

This command is configure the packets proportion of the appointed class for the weight fair mechanism. The switch contains n+1 hardware priority queues. Incoming packets must be mapped to one of these n+1 queues. This command is used to configure the maximum number of packets each hardware priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets.

Parameters

Parameters	Description
class_id	Specify which of the n+1 hardware priority queues the config scheduling command will apply to. The four hardware priority queues are identified by number – from 0 to n – with the 0 queue being the lowest priority.
max_packet	Specify the maximum number of packets the priority queue will be allowed to transmit before allowing the next lowest priority queue to transmit its packets. A value between 0 and 255 can be specified.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the traffic scheduling mechanism for each Class 0 OS queue:

```
DGS-3200-10:4# config scheduling 0 max_packet 34
Command: config scheduling 0 max_packet 34

Success.

DGS-3200-10:4#
```

67-6 config scheduling_mechanism

Purpose

To configure the traffic scheduling mechanism for each COS queue.

Format

config scheduling_mechanism [strict | weight_fair]

Description

This command is used to specify how the switch handle packets in priority queues.

Parameters

Parameters	Description
strict	The highest queue should process first. That is, the highest queue should be finished first.
weight_fair	Use weighted fair algorithm to handle packets in priority queues.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3200-10:4#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.

DGS-3200-10:4#
```

67-7 show scheduling

Purpose

To display the current traffic scheduling parameters in use on the switch.

Format

show scheduling

Description

This command is used to display the current traffic scheduling parameters in use on the switch.

Parameters

None.

Restrictions

None.

Examples

To display traffic scheduling parameters for each COS queue (for ex., eight hardware priority queues):

```
DGS-3200-10:4# show scheduling
Command: show scheduling

QOS Output Scheduling

Class ID  MAX. Packets
--------  ------------
Class-0  1
Class-1  2
Class-2  3
Class-3  4
Class-4  5
Class-5  6
Class-6  7
Class-7  8

DGS-3200-10:4#
```

67-8 show scheduling_mechanism

Purpose

To show the traffic scheduling mechanism.

Format

show scheduling_mechanism

Description

This command is used to display the traffic scheduling mechanism.

Parameters

None.

Restrictions

None.

Examples

To show the scheduling mechanism:

```
DGS-3200-10:4# show scheduling_mechanism
Command: show scheduling_mechanism

QOS scheduling mechanism
CLASS ID  Mechanism
--------  -----------
Class-0   strict
Class-1   strict
Class-2   strict
Class-3   strict
Class-4   strict
Class-5   strict
Class-6   strict
Class-7   strict

DGS-3200-10:4#
```

67-9 config 802.1p user_priority

Purpose

To map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the switch.

Format

config 802.1p user_priority <priority 0-7> <class_id 0-7>

Description

This command is used to configure the way the switch will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the switch. The switch's default is to map the incoming 802.1p user priority values to one of the eight hardware priority queues.

Parameters

Parameters	Description
priority	The 802.1p user priority you want to associate with the **<class_id>** (the number of the hardware queue).
class_id	The number of the switch's hardware priority queue. The switch has eight hardware priority queues available.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 802.1p user priority:

```
DGS-3200-10:4# config 802.1p user_priority 1 3
Command: config 802.1p user_priority 1 3

Success.

DGS-3200-10:4#
```

67-10 show 802.1p user_priority

Purpose

To display 802.1p user priority.

Format

show 802.1p user_priority

Description

This command is used to display 802.1p user priority.

Parameters

None.

Restrictions

None.

Examples

To display the traffic scheduling mechanism for each COS queue:

```
DGS-3200-10:4# show 802.1p user_priority
Command: show 802.1p user_priority

QOS Class of Traffic
Priority-0  ->  <Class-2>
Priority-1  ->  <Class-0>
Priority-2  ->  <Class-1>
Priority-3  ->  <Class-3>
Priority-4  ->  <Class-4>
Priority-5  ->  <Class-5>
Priority-6  ->  <Class-6>
Priority-7  ->  <Class-7>

DGS-3200-10:4#
```

67-11 config 802.1p default_priority

Purpose

To configure the 802.1p default priority settings on the switch. If an untagged packet is received by the switch, the priority configured with this command will be written to the packet's priority field.

Format

config 802.1p default_priority [<portlist> | all] <priority 0-7>

Description

This command is used to specify default priority handling of untagged packets received by the switch. The priority value entered with this command will be used to determine which of the four hardware priority queues the packet is forwarded to.

Parameters

Parameters	Description
portlist	Specify a range of ports for which the default priority is to be configured. That is, a range of ports for which all untagged packets received will be assigned the priority specified below. The beginning and end of the port list range are separated by a dash.
all	Specify that the command applies to all ports on the switch.
priority	The priority value (0 to 7) you want to assign to untagged packets received by

	the switch or a range of ports on the switch.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the 802.1p default priority settings on the switch:

```
DGS-3200-10:4#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3200-10:4#
```

67-12 show 802.1p default_priority

Purpose

To display the current default priority settings on the switch.

Format

show 802.1p default_priority { <portlist> }

Description

This command is used to display the current default priority settings on the switch. If no parameter is specified, the system will display all ports with 802.1p **default_priority**.

Parameters

Parameters	Description
portlist	Specify a range of ports to be displayed.

Restrictions

None.

Examples

To display 802.1p default priority:

```
DGS-3200-10:4# show 802.1p default_priority
Command: show 802.1p default_priority

Port        Priority      Effective Priority
----        -----------   ------------------
1               0                       0
2               0                       0
3               0                       0
4               0                       0
5               0                       0
6               0                       0
7               0                       0
8               0                       0
9               0                       0
10           0                  0

DGS-3200-10:4#
```

X. IP Addressing Service

The IP Addressing Service section includes the following chapters: DHCP Server, DHCP Relay, DHCP Local Relay, DNS Resover and PPPoE Circuit ID Insertions.

68 DHCP Server Command List

create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>
delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> | all]
show dhcp excluded_address
create dhcp pool <pool_name 12>
delete dhcp pool [<pool_name 12>|all]
config dhcp pool network_addr <pool_name 12> <network_address>
config dhcp pool domain_name <pool_name 12> {<domain_name 64>}
config dhcp pool dns_server <pool_name 12> {<ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool netbios_name_server <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]
config dhcp pool default_router <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}
config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]
config dhcp pool boot_file <pool_name 12> {<file_name 64>}
config dhcp pool next_server <pool_name 12> {< ipaddr>}
config dhcp ping_packets <number 0-10>
config dhcp ping_timeout <millisecond 10-2000>
create dhcp pool manual_binding <pool_name 12> < ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}
delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]
clear dhcp binding [<pool_name 12>[<ipaddr> | all] | all]
show dhcp binding { <pool_name 12>}
show dhcp pool { <pool_name 12>}
show dhcp pool manual_binding { <pool_name 12>}
enable dhcp_server
disable dhcp_server
show dhcp_server
clear dhcp conflict_ip [<ipaddr> | all]
show dhcp conflict_ip {<ipaddr>}

68-1 create dhcp excluded_address

Purpose

To specify the IP addresses that the DHCP server should not assign to a DHCP client.

Format

create dhcp excluded_address begin_address <ipaddr> end_address <ipaddr>

Description

This command is used to create a DHCP server exclude address. The DHCP server assumes that all IP addresses in a DHCP pool subnet are available for assigning to DHCP clients. Use this command to specify the IP address that the DHCP server should not assign to clients. This command can be used multiple times in order to define multiple groups of excluded addresses.

Parameters

Parameters	Description
<ipaddr>	Specify start and end address of IP address range.

Restrictions

Only Administrator-level users can issue this command.

Examples

To specify the IP address that the DHCP server should not assign to a client:

```
DGS-3200-10:4# create dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10
Command: create dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DGS-3200-10:4#
```

68-2 delete dhcp excluded_address

Purpose

To delete an excluded address off the DHCP server.

Format

delete dhcp excluded_address [begin_address <ipaddr> end_address <ipaddr> | all]

Description

This command is used to delete a DHCP server exclude address.

Parameters

Parameters	Description
<ipaddr>	Specify start and end address of IP address range.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a DHCP server exclude address:

```
DGS-3200-10:4#delete dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10
Command: delete dhcp excluded_address begin_address 10.10.10.1 end_address 10.10.10.10

Success.

DGS-3200-10:4#
```

68-3 show dhcp excluded_address

Purpose

To display the groups of IP addresses which are excluded from the legal assigned IP address.

Format

show dhcp excluded_address

Description

This command is used to display the groups of IP addresses which are excluded from the legal assigned IP address.

Parameters

None.

Restrictions

None.

Examples

To display the DHCP server excluded addresses:

```
DGS-3200-10:4#show dhcp excluded_address
Command: show dhcp excluded_address

Index  Begin Address    End Address
-----  ---------------  ---------------
1      192.168.0.1      192.168.0.100
2      10.10.10.10      10.10.10.10

Total Entries : 2

DGS-3200-10:4#
```

68-4 create dhcp pool

Purpose

To create a DHCP pool.

Format

create dhcp pool <pool_name 12>

Description

This command is used to create a DHCP pool by specifying a name. After creating a DHCP pool, use other DHCP pool configuration commands to configure parameters for the pool.

Parameters

Parameters	Description
<pool_name 12>	Specify the name of the DHCP pool.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a DHCP pool:

```
DGS-3200-10:4#create dhcp pool nyknicks
Command: create dhcp pool nyknicks

Success.


DGS-3200-10:4#
```

68-5 delete dhcp pool

Purpose

To delete a DHCP pool.

Format

delete dhcp pool [<pool_name 12>|all]

Description

This command is used to delete a DHCP pool.

Parameters

Parameters	Description
<pool_name 12>	Specify the name of the DHCP pool.
all	Specify to delete all the DHCP pools.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a DHCP pool:

```
DGS-3200-10:4#delete dhcp pool nyknicks
Command: delete dhcp pool nyknicks

Success.

DGS-3200-10:4#
```

68-6 config dhcp pool network_addr

Purpose

To specify the network address for the DHCP pool.

Format

config dhcp pool network_addr <pool_name 12> <network_address>

Description

This command is used to specify the network for the DHCP pool. The addresses in the network are free to be assigned to the DHCP client. The prefix length specifies the number of bits that comprise the address prefix. The prefix is an alternative way of specifying the network mask of the client. The prefix length must be preceded by a forward slash (/). When the DHCP server receives a request from the client, the server will automatically find a pool to allocate the address. If the request is relayed to the server by the

intermediate device, the server will match the gateway IP address carried in the packet against the network of each DHCP pool. The pool which has the longest match will be selected. If the request packet is not through relay, then the server will match the IP address of the IPIF that received the request packet against the network of each DHCP pool.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<network_address>	Specify the IP address that the DHCP server may assign to clients.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the address range of the DHCP address pool:

```
DGS-3200-10:4# config dhcp pool network_addr nyknicks 10.10.10.0/24
Command: config dhcp pool network_addr nyknicks 10.10.10.0/24

Success.

DGS-3200-10:4#
```

68-7 config dhcp pool domain_name

Purpose

To specify the domain name for the client if the server allocates the address for the client from this pool.

Format

config dhcp pool domain_name <pool_name 12> {<domain_name 64>}

Description

This command is used to specify the domain name for the client if the server allocates the address for the client from this pool. The domain name configured here will be used as the default domain name by the client. By default, the domain name is empty. If the domain name is empty, the domain name information will not be provided to the client.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<domain_name 64>	Specify the domain name of the client.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the domain name option of the DHCP pool:

```
DGS-3200-10:4# config dhcp pool domain_name nyknicks nba.com
Command: config dhcp pool domain_name nyknicks nba.com

Success.

DGS-3200-10:4#
```

68-8 config dhcp pool dns_server

Purpose

To specify the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified in one command line.

Format

config dhcp pool dns_server <pool_name 12> {<ipaddr>} {< ipaddr>} {< ipaddr>}

Description

This command is used to specify the IP address of a DNS server that is available to a DHCP client. Up to three IP addresses can be specified on one command line. If DNS server is not specified, the DNS server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP poll name.
<ipaddr>	Specify the IP address of the DNS server. Up to three IP addresses can be specified on one command line.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DNS server's IP address of the DHCP pool:

```
DGS-3200-10:4#config dhcp pool dns_server nyknicks 10.10.10.1
Command: config dhcp pool dns_server nyknicks 10.10.10.1

Success.

DGS-3200-10:4#
```

68-9 config dhcp pool netbios_name_server

Purpose

To specify the NetBIOS WINS server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified in one command line.

Format

config dhcp pool netbios_name_server <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}

Description

This command is used to specify the NetBIOS WINS server that is available to a Microsoft DHCP client. Up to three IP addresses can be specified on one command line.

Windows Internet Naming Service (WINS) is a name resolution service that Microsoft DHCP clients use to correlate host names to IP addresses within a general grouping of networks. If a NetBIOS name server is not specified, the NetBIOS name server information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP poll name.
<ipaddr>	Specify the IP address of the WINS server. Up to three IP addresses can be specified on one command line.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure WINS server's IP address of the DHCP pool:

```
DGS-3200-10:4#config dhcp pool netbios_name_server knicks 10.10.10.1
Command: config dhcp pool netbios_name_server knicks 10.10.10.1

Success.

DGS-3200-10:4#
```

68-10 config dhcp pool netbios_node_type

Purpose

To specify the NetBIOS node type for a Microsoft DHCP client.

Format

config dhcp pool netbios_node_type <pool_name 12> [broadcast | peer_to_peer | mixed | hybrid]

Description

This command is used to specify the NetBIOS node type for a Microsoft DHCP client.

The NetBIOS node type for Microsoft DHCP clients can be one of four settings: broadcast, peer-to-peer, mixed, or hybrid. Use this command to configure a NetBIOS over TCP/IP device that is described in RFC 1001/1002. By default, the NetBIOS node type is broadcast.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<node_type>	NetBIOS node type for a Microsoft DHCP client.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure NETBIOS node type of the DHCP pool:

```
DGS-3200-10:4#config dhcp pool netbios_node_type knicks hybrid
Command: config dhcp pool netbios_node_type knicks hybrid

Success.

DGS-3200-10:4#
```

68-11 config dhcp pool default_router

Purpose

To specify the IP address of the default router for a DHCP client. Up to three IP addresses can be specified in one command line.

Format

config dhcp pool default_router <pool_name 12> {< ipaddr>} {< ipaddr>} {< ipaddr>}

Description

This command is used to specify the IP address of the default router for a DHCP client. Up to three IP addresses can be specified on one command line. After a DHCP client has booted, the client begins sending packets to its default router. The IP address of the default router should be on the same subnet as the client. If the default router is not specified, the default router information will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command. The default router must be within the range the network defined for the DHCP pool.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<ipaddr>	Specify the IP address of the default router. Up to three IP addresses can be specified on one command line.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure default router of the DHCP pool:

```
DGS-3200-10:4#config dhcp pool default_router nyknicks 10.10.10.1
Command: config dhcp pool default_router nyknicks 10.10.10.1

Success.

DGS-3200-10:4#
```

68-12 config dhcp pool lease

Purpose

To specify the duration of the lease.

Format

config dhcp pool lease <pool_name 12> [<day 0-365> <hour 0-23> <minute 0-59> | infinite]

Description

This command is used to specify the duration of the DHCP pool lease. By default, each IP address assigned by a DHCP server comes with a one-day lease, which is the amount of time that the address is valid.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool's name.
<day 0-365>	Specify the number of days of the lease.
<hour 0-23>	Specify the number of hours of the lease.
<minute 0-59>	Specify the number of minutes of the lease.
infinite	Specify a lease of unlimited duration.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure lease of a pool:

```
DGS-3200-10:4#config dhcp pool lease nyknicks infinite
Command: config dhcp pool lease nyknicks infinite

Success.

DGS-3200-10:4#
```

68-13 config dhcp pool boot_file

Purpose

To specify the name of the file that is used as a boot image.

Format

config dhcp pool boot_file <pool_name 12> {<file_name 64>}

Description

This command is used to specify the name of the file that is used as a boot image. The boot file is used to store the boot image for the client. The boot image is generally the operating system the client uses to load. If this command is input twice for the same pool, the second command will overwrite the first command. If the bootfile is not specified, the boot file information will not be provided to the client.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<file_name 64>	Specify the file name of the boot image.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure boot file of the DHCP pool:

```
DGS-3200-10:4#config dhcp pool boot_file engineering boot.had
Command: config dhcp pool boot_file engineering boot.had

Success.

DGS-3200-10:4#
```

68-14 config dhcp pool next_server

Purpose

To specify the next server to be used in the DHCP client boot process.

Format

config dhcp pool next_server <pool_name 12> {< ipaddr>}

Description

This command is used by the DHCP client boot process, typically a TFTP server. If next server information is not specified, it will not be provided to the client. If this command is input twice for the same pool, the second command will overwrite the first command.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<ipaddr>	Specify the IP address of the next server.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure next server of the DHCP pool:

```
DGS-3200-10:4#config dhcp pool next_server engineering 192.168.0.1
Command: config dhcp pool next_server engineering 192.168.0.1

Success.

DGS-3200-10:4#
```

68-15 config dhcp ping_packets

Purpose

To specify the number of ping packets the DHCP server sends to the IP address before assigning this address to a requesting client.

Format

config dhcp ping_packets <number 0-10>

Description

This command is used to specify the number of ping packets the DHCP server sends to an IP address before assigning this address to a requesting client. By default, the DHCP server pings a pool address twice before assigning the address to a DHCP client. If the ping is unanswered, the DHCP server assumes (with a high probability) that the address is not in use and assigns the address to the requesting client. If the ping is answered, the server will discard the current IP address and try another IP address.

Parameters

Parameters	Description
<number 0-10>	Specify the number of ping packets. 0 means there is no ping test. The default value is 2.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure ping packets of the DHCP server:

```
DGS-3200-10:4# config dhcp ping_packets 4
Command: config dhcp ping_packets 4

Success.

DGS-3200-10:4#
```

68-16 config dhcp ping_timeout

Purpose

To specify the amount of time the DHCP server must wait before timing out a ping packet.

Format

config dhcp ping_timeout <millisecond 10-2000>

Description

This command is used to specify the amount of time the DHCP server must wait before timing out a ping packet. By default, the DHCP server waits 100 milliseconds before timing out a ping packet.

Parameters

Parameters	Description
<millisecond 10-2000>	Specify the amount of time the DHCP server must wait before timing out a ping packet. The default value is 100.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the time out value for ping packets of the DHCP server:

```
DGS-3200-10:4#config dhcp ping_timeout 500
Command: config dhcp ping_timeout 500

Success.

DGS-3200-10:4#
```

68-17 create dhcp pool manual_binding

Purpose

To create the manual binding for the DHCP pool.

Format

create dhcp pool manual_binding <pool_name 12> < ipaddr> hardware_address <macaddr> {type [ethernet | ieee802]}

Description

This command is used to specify the distinct identification of the client in dotted-hexadecimal notation or hardware address.

An address binding is a mapping between the IP address and MAC address of a client. The IP address of a client can be assigned manually by an administrator or assigned automatically from a pool by a DHCP server.

The IP address specified in the manual binding entry must be in a range within that the network uses for the DHCP pool. If the user specifies a conflict IP address, an error message will be returned. If a number of manual binding entries are created, and the network address for the pool is changed such that conflicts are

generated, those manual binding entries which conflict with the new network address will be automatically deleted.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<ipaddr>	Specify the IP address which will be assigned to a specified client.
<macaddr >	Specify the hardware MAC address.
type	Specify **ethernet** or **ieee802** as the DHCP pool manual binding type.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure manual bindings for the DHCP pool:

```
 DGS-3200-10:4#create dhcp pool manual_binding engineering 10.10.10.1 hardware_address
00-80-C8-02-02-02 type ethernet
 Command: create dhcp pool manual_binding engineering 10.10.10.1 hardware_address
00-80-C8-02-02-02 type ethernet

 Success.

 DGS-3200-10:4#
```

68-18 delete dhcp pool manual_binding

Purpose

To delete one or all manual binding of the specified DHCP pool.

Format

delete dhcp pool manual_binding <pool_name 12> [<ipaddr> | all]

Description

This command is used to delete DHCP server manual binding.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name.
<ipaddr>	Specify the IP address which will be assigned to a specified client.
all	Specify to delete all IP addresses.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a manual binding from the DHCP pool:

```
DGS-3200-10:4#delete dhcp pool manual_binding engineering 10.10.10.1
Command: delete dhcp pool manual_binding engineering 10.10.10.1

Success.

DGS-3200-10:4#
```

68-19 clear dhcp binding

Purpose

To delete all the dynamic binding entries for a pool or all pools.

Format

clear dhcp binding [<pool_name 12>[<ipaddr> | all] | all]

Description

This command clears a binding entry or all binding entries in a pool or clears all binding entries in all pools.

Note that this command will not clear the dynamic binding entry which matches a manual binding entry.

Parameters

Parameters	Description
<pool_name 12>	Specify the DHCP pool name to clear.
all	Specify to clear all binding entries.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear dynamic binding entries in the pool named “engineering”:

```
DGS-3200-10:4# clear dhcp binding engineering 10.20.3.4
Command: clear dhcp binding engineering 10.20.3.4

Success.

DGS-3200-10:4#
```

68-20 show dhcp binding

Purpose

To display the current binding entry information.

Format

show dhcp binding { <pool_name 12>}

Description

This command is used to display dynamic binding entries.

Parameters

Parameters	Description
<pool_name 12>	Specify a DHCP pool name.

Restrictions

None.

Examples

To display the current binding entries for “engineering”:

```
DGS-3200-10:4#show dhcp binding engineering
Command: show dhcp binding engineering

Pool Name    IP Addresss   Hardware Address   Type     Status   Lifetime
-----------  ------------- ----------------- --------  -------  ---------
engineering  192.168.0.1   00-80-C8-08-13-88  Ethernet  Manual   86400
engineering  192.168.0.2   00-80-C8-08-13-99  Ethernet  Automatic 86400
engineering  192.168.0.3   00-80-C8-08-13-A0  Ethernet  Automatic 86400
engineering  192.168.0.4   00-80-C8-08-13-B0  Ethernet  Automatic 86400

Total Entries: 4

DGS-3200-10:4#
```

68-21 show dhcp pool

Purpose

To display the information for a DHCP pool.

Format

show dhcp pool { <pool_name 12>}

Description

This command is used to display the information for a DHCP pool.

Parameters

Parameters	Description
<pool_name 12>	Specify a DHCP pool name.

Restrictions

None.

Examples

To display the current DHCP pool information for “engineering”:

```
DGS-3200-10:4# show dhcp pool engineering
Command: show dhcp pool engineering

Pool Name        : engineering
Network Address   : 10.10.10.0/24
Domain Name      : dlink.com
DNS Server       : 10.10.10.1
NetBIOS Name Server : 10.10.10.1
NetBIOS Node Type : Broadcast
Default Router    : 10.10.10.1
Pool Lease       : 10 Days, 0 Hours, 0 Minutes
Boot File        : boot.bin
Next Server      : 10.10.10.2

DGS-3200-10:4#
```

68-22 show dhcp pool manual_binding

Purpose

To display the configured manual binding entries.

Format

show dhcp pool manual_binding { <pool_name 12>}

Description

This command is used to display the configured manual binding entries.

Parameters

Parameters	Description
<pool_name 12>	Specify a DHCP pool name.

Restrictions

None.

Examples

To display the configured manual binding entries:

```
DGS-3200-10:4# show dhcp pool manual_binding
Command: show dhcp pool manual_binding

Pool Name    IP Address    Hardware Address   Type
------------ ------------- ------------------ --------
p1          192.168.0.1   00-80-C8-08-13-88  Ethernet
p1          192.168.0.2   00-80-C8-08-13-99  Ethernet

Total Entries : 2

DGS-3200-10:4#
```

68-23 enable dhcp_server

Purpose

To enable the DHCP server function.

Format

enable dhcp_server

Description

This command is used to enable the DHCP server function. If DHCP relay is enabled, DHCP server cannot be enabled. The opposite is also true. For Layer 2 switches, if DHCP client is enabled on the only interface, then DHCP server cannot be enabled. For layer 3 switches, when the System interface is the only interface then can DHCP client be enabled. If the DHCP client is enabled, then the DHCP server cannot be enabled.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable DHCP server:

```
DGS-3200-10:4# enable dhcp_server
Command: enable dhcp_server

Success.

DGS-3200-10:4#
```

68-24 disable dhcp_server

Purpose

To disable the DHCP server function on the Switch.

Format

disable dhcp_server

Description

This command is used to disable the DHCP server function on the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the Switch's DHCP server:

```
DGS-3200-10:4#disable dhcp_server
Command: disable dhcp_server

Success.

DGS-3200-10:4#
```

68-25 show dhcp_server

Purpose

To display the current DHCP server configuration.

Format

show dhcp_server

Description

This command is used to display the current DHCP server configuration.

Parameters

None.

Restrictions

None.

Examples

To display the DHCP server status:

```
DGS-3200-10:4#show dhcp_server
Command: show dhcp_server

  DHCP Server Global State: Disabled
  Ping Packet Number     : 2
  Ping Timeout          : 100 ms

DGS-3200-10:4#
```

68-26 clear dhcp conflict_ip

Purpose

To clear an entry or all entries from the conflict IP database.

Format

clear dhcp conflict_ip [<ipaddr> | all]

Description

This command is used to clear an entry or all entries from the conflict IP database.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address to be cleared.
all	Specify that all IP addresses will be cleared.

Restrictions

Only Administrator-level users can issue this command.

Examples

To clear an IP address 10.20.3.4 from the conflict database:

```
DGS-3200-10:4# clear dhcp conflict_ip 10.20.3.4
Command: clear dhcp conflict_ip 10.20.3.4

Success.

DGS-3200-10:4#
```

68-27 show dhcp conflict_ip

Purpose

To display the IP address that has been identified as being in conflict.

Format

show dhcp conflict_ip {<ipaddr>}

Description

This command is used to display the IP address that has been identified as being in conflict. The DHCP server will use ping packet to determine whether an IP address is conflicting with other hosts before binding this IP. The IP address which has been identified in conflict will be moved to the conflict IP database. The system will not attempt to bind the IP address in the conflict IP database unless the user clears it from the conflict IP database.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address to be displayed.

Restrictions

None.

Examples

To display the entries in the DHCP conflict IP database:

```
DGS-3200-10:4# show dhcp conflict_ip
Command: show dhcp conflict_ip

 IP Address    Detection Method   Detection Time
-----------   ----------------   --------------------
172.16.1.32   Ping                 2007/08/30 17:06:59
172.16.1.32   Gratuitous ARP     2007/09/10 19:38:01

DGS-3200-10:4#
```

69 DHCP Relay Command List

config dhcp_relay { hops <value 1-16> | time <sec 0-65535>}
config dhcp_relay [add|delete] ipif <ipif_name 12> <ipaddr>
config dhcp_relay option_82 {state [enable|disable] | check [enable|disable] | policy [replace|drop|keep] | remote_id [default | user_define <desc 32>]}
enable dhcp _relay
disable dhcp _relay
show dhcp _relay {ipif <ipif_name 12>}

Note: 1. The DHCP relay commands include all the commands defined in the BOOTP relay command section; If this DHCP relay command set is supported in your system, the BOOTP relay commands can be ignored.

2. The system supporting DHCP relay will accept BOOTP relay commands in the config file but not allow input from the console screen, and these BOOTP relay commands setting from the config file will be saved as DHCP relay commands while the save command is performed.

69-1 config dhcp_relay

Purpose

To configure the DHCP relay feature of the switch.

Format

config dhcp_relay { hops <value 1-16> | time <sec 0-65535>}

Description

This command is used to configure the DHCP relay feature of the switch.

Parameters

Parameters	Description
hops	Specify the maximum number of router hops that the DHCP/BOOTP packets can cross. The range is 1 to 16. The default value is 4.
time	The minimum time in seconds within which the switch must relay the DHCP/BOOTP request. If this time is exceeded, the switch will drop the DHCP/BOOTP packet. The range is 0 to 65535. The default value is 0.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure DHCP relay status:

```
DGS-3200-10:4#config dhcp_relay hops 4 time 2
Command: config dhcp_relay hops 4 time 2

Success.

DGS-3200-10:4#
```

69-2 config dhcp_relay add

Purpose

To add an IP destination address to the switch's DHCP relay table.

Format

config dhcp_relay add ipif <ipif_name 12> <ipaddr>

Description

This command is used to add an IP address as a destination to forward (relay) DHCP/BOOTP packets.

Parameters

Parameters	Description
ipif_name	The name of the IP interface which contains the IP address below.
ipaddr	The DHCP/BOOTP server IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a DHCP/BOOTP server to the relay table:

```
DGS-3200-10:4#config dhcp_relay add ipif System 10.43.21.12
Command: config dhcp_relay add ipif System 10.43.21.12

Success.

DGS-3200-10:4#
```

69-3 config dhcp_relay delete

Purpose

To delete one or all IP destination addresses from the switch's DHCP relay table.

Format

config dhcp_relay delete ipif <ipif_name 12> <ipaddr>

Description

This command is used to delete one or all of the IP destination addresses in the switch's relay table.

Parameters

Parameters	Description
ipif_name	The name of the IP interface which contains the IP address below.
ipaddr	The DHCP/BOOTP server IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a DHCP/BOOTP server to the relay table:

```
DGS-3200-10:4#config dhcp_relay delete ipif System 10.43.21.12
Command: config dhcp_relay delete ipif System 10.43.21.12

Success.

DGS-3200-10:4#
```

69-4 config dhcp_relay option_82

Purpose

To configure the DHCP relay agent information option 82 of the switch.

Format

config dhcp_relay option_82 {state [enable|disable] | check [enable|disable] | policy [replace|drop|keep] | remote_id [default | user_define <desc 32>]}

Description

This command is used to configure the DHCP relay agent information option 82 setting of the switch.

The formats for the circuit ID suboption and the remote ID suboption are indicated in the following diagram.

For the circuit ID suboption of a standalone switch, the module field is always zero.

Circuit ID suboption format :

1.	2.	3.	4.	5.	6.	7.
1	6	0	4	VLAN	Module	Port
1 byte	1 byte	1 byte	1 byte	2 bytes	1 byte	1 byte

1. Suboption type 2. Length

3. Circuit ID type 4. Length

5. VLAN : The incoming VLAN ID of DHCP client packet.

6 . Module : For a standalone switch, Module is always 0.

7. Port : The incoming port number of DHCP client packet, port number starts from 1.

Remote ID suboption format :

1.	2.	3.	4.	5.
2	8	0	6	MAC address
1 byte	1 byte	1 byte	1 byte	6 bytes

1. Suboption type 2. Length

3. Remote ID type 4. Length

5. MAC address : The switch's system MAC address.

Parameters

Parameters	Description
state	Enable or disable the switch to insert and remove DHCP relay agent information 82 field in messages between DHCP server and client. The default setting is **disable**.
check	Enable or disable the switch to check the validity of DHCP relay agent information 82 field in messages between DHCP server and client. The invalid messages are those packets that contain the option 82 field from DHCP client and those packets that contain the wrong format of option 82 field from DHCP server. If check is set to enable, the switch will drop all invalid messages received from DHCP server or client. The default setting is **disable**.
policy	Configure the reforwarding policy as follows : **replace**: replace the exiting option 82 field in messages. **drop**: discard messages with existing option 82 field. **keep**: retain the existing option 82 field in messages. The default setting is replace. Note: The reforwarding policy is active only when the "check" option is disabled.
remote_id	Specify the content in the Remote ID sub-option. **default** - Use the Switch's system MAC address as the remote ID. **user_define** - Use the user-defined string as the remote ID. Space char is allowed in the string.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DHCP relay option 82:

```
DGS-3200-10:4#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3200-10:4#config dhcp_relay option_82 check disable
Command: config dhcp_relay option_82 check disable

Success.

DGS-3200-10:4#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3200-10:4#
```

69-5 enable dhcp_relay

Purpose

To enable the DHCP relay function on the switch.

Format

enable dhcp_relay

Description

This command is used to enable the DHCP relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the DHCP relay function:

```
DGS-3200-10:4#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3200-10:4#
```

69-6 disable dhcp_relay

Purpose

To disable DHCP relay function on the switch.

Format

disable dhcp_relay

Description

This command is used to disable the DHCP relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the DHCP relay function:

```
DGS-3200-10:4#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3200-10:4#
```

69-7 show dhcp_relay

Purpose

To display the current DHCP relay configuration.

Format

show dhcp_relay {ipif <ipif_name 12>}

Description

This command is used to display the current DHCP relay configuration. If no parameter is specified , the system will display all DHCP relay configurations.

Parameters

Parameters	Description
ipif_name	The IP interface name.

Restrictions

None.

Examples

To display the DHCP relay status:

```
DGS-3200-10:4# show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/BOOTP Relay Status         : Disabled
DHCP/BOOTP Hops Count Limit     : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace
DHCP Relay Agent Information Option 82 Remote ID : 00-24-01-15-1C-96

Interface     Server 1        Server 2         Server 3        Server 4
------------- --------------- ---------------- --------------- --------------
System        10.48.74.122    10.23.12.34      10.12.34.12     10.48.75.121

DGS-3200-10:4#
```

70 DHCP Local Relay Command List

config dhcp_local_relay vlan <vlan_name 32> state [enable|disable]
enable dhcp _local_relay
disable dhcp_relay_relay
show dhcp _local_relay
config dhcp_local_relay option_82 ports <portlist> policy [replace | drop | keep]
show dhcp_local_relay option_82 ports {<portlist>}

70-1 config dhcp_local_relay vlan

Purpose

To enable or disable the DHCP local relay function for a specific VLAN.

Format

config dhcp_local_relay vlan <vlan_name 32> state [enable|disable]

Description

This command is used to enable or disable the DHCP local relay function for a specified VLAN. When DHCP local relay is enabled for the VLAN, the DHCP packet will be relayed as a broadcast without changing the source MAC address and gateway address. DHCP option 82 will be automatically added.

Parameters

Parameters	Description
vlan_name	The name of the VLAN to be enabled for DHCP local relay.
state	Enable or disable DHCP local relay for a specified VLAN.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable DHCP local relay for a default VLAN:

```
DGS-3200-10:4#config dhcp_local_relay vlan default state enable
Command: config dhcp_local_relay vlan default state enable

Success.

DGS-3200-10:4#
```

70-2 enable dhcp_local_relay

Purpose

To enable DHCP local relay.

Format

enable dhcp_local_relay

Description

This command is used to enable the DHCP local relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the DHCP local relay function:

```
DGS-3200-10:4#enable dhcp_local_relay
Command: enable dhcp_local_relay


Success.


DGS-3200-10:4#
```

70-3 disable dhcp_local_relay

Purpose

To disable the DHCP local relay function.

Format

disable dhcp_local_relay

Description

This command is used to disable the DHCP local relay function on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To disable the DHCP local relay function:

```
DGS-3200-10:4#disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.

DGS-3200-10:4#
```

70-4 show dhcp_local_relay

Purpose

To display the current DHCP local relay configuration.

Format

show dhcp_local_relay

Description

This command is used to display the current DHCP local relay configuration on the switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To display the local DHCP relay status:

```
DGS-3200-10:4#show dhcp_local_relay
Command: show dhcp_local_relay



DHCP/BOOTP Local Relay Status          : Disabled
DHCP/BOOTP Local Relay VID List        : 1,3-4

DGS-3200-10:4#
```

70-5 config dhcp_local_relay option_82

Purpose

To configure DHCP local relay each port processing option 82 policy.

Format

config dhcp_local_relay option_82 ports <portlist> policy [replace | drop | keep]

Description

This command is used to configure the processing of DHCP 82 option for the DHCP local relay function with each port.

Parameters

Parameters	Description
ports	Specify specific ports' option82 policy of processing the received DHCP packets.
policy	Specifies how to process the packets coming from the client side which have the option 82 field. **replace** - Replace the exiting option 82 field in the packet. **drop** - Discard if the packet has the option 82 field. **keep** - Retain the existing option 82 field in the packet.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure port 1-3 DHCP local relay option 82 policy to replace:

```
DGS-3200-10:4# config dhcp_local_relay option_82 ports 1-3 policy replace
Command: config dhcp_local_relay option_82 ports 1-3 policy replace

Success.

DGS-3200-10:4#
```

70-6 show dhcp_local_relay option_82

Purpose

To display the current DHCP local relay option82 configuration of each port.

Format

show dhcp_local_relay option_82 ports {<portlist>}

Description

This command is used to display the current DHCP local relay option82 configuration of each port.

Parameters

Parameters	Description
<portlist>	Specify a list of ports to show their option82 policy.

Restrictions

None.

Examples

To display DHCP local relay option82 configuration of each port:

```
DGS-3200-10:4#show dhcp_local_relay option_82 ports
Command: show dhcp_local_relay option_82 ports

Port  Option 82
      Policy
----  ---------
1     replace
2     replace
3     replace
4     keep
5     keep
6     keep
7     keep
8     keep
9     keep
10    keep

DGS-3200-10:4#
```

71 Domain Name System (DNS) Resolver Command List

config name_server add <ipaddr> {primary}
config name_server delete <ipaddr> {primary}
config name_server timeout <sec 1-60>
show name_server
create host_name <name 255> <ipaddr>
delete host_name [<name 255> | all]
show host_name {static | dynamic}
enable dns_resolver
disable dns_resolver

71-1 config name_server add

Purpose

To add a DNS resolver name server to the Switch.

Format

config name_server add <ipaddr> {primary}

Description

This command is used to add a DNS resolver name server to the Switch.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the DNS Resolver name server.
primary	Specify the name server as a primary name server.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add DNS Resolver primary name server 10.10.10.10:

```
DGS-3200-10:4# config name_server add 10.10.10.10 primary
Command: config name_server add 10.10.10.10 primary


Success.


DGS-3200-10:4#
```

71-2 config name_server delete

Purpose

To delete a DNS resolver name server from the Switch.

Format

config name_server delete <ipaddr> {primary}

Description

This command is used to delete a DNS resolver name server from the Switch.

Parameters

Parameters	Description
<ipaddr>	Specify the IP address of the DNS Resolver name server.
primary	Specify the name server as a primary name server.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete DNS Resolver name server 10.10.10.10:

```
DGS-3200-10:4# config name_server delete 10.10.10.10
Command: config name_server delete 10.10.10.10

Success.

DGS-3200-10:4#
```

71-3 config name_server timeout

Purpose

To configure the timeout value of a DNS Resolver name server.

Format

config name_server timeout <sec 1-60>

Description

This command is used to configure the timeout value of a DNS Resolver name server.

Parameters

Parameters	Description
<sec 1-60>	Specify the maximum time waiting for a response from a specified name server.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure DNS Resolver name server time out to 10 seconds:

```
DGS-3200-10:4# config name_server timeout 10
Command: config name_server timeout 10

Success.

DGS-3200-10:4#
```

71-4 show name_server

Purpose

To display the current DNS Resolver name servers and name server time out on the Switch.

Format

show name_server

Description

This command is used to display the current DNS Resolver name servers and name server time out on the Switch.

Parameters

None.

Restrictions

None.

Examples

To display the current DNS Resolver name servers and name server time out:

```
DGS-3200-10:4# show name_server
Command: show name_server

Name Server Time Out: 3 seconds

Static Name Server Table:
Server IP Address     Priority
--------------------- --------------
20.20.20.20             Secondary
10.1.1.1                Primary

Dynamic Name Server Table:
Server IP Address     Priority
--------------------- --------------
10.48.74.122            Primary

DGS-3200-10:4#
```

71-5 create host_name

Purpose

To create the static host name entry of the Switch.

Format

create host_name <name 255> <ipaddr>

Description

This command is used to create the static host name entry of the Switch.

Parameters

Parameters	Description
<name 255>	Enter the hostname up to 255 characters long.
<ipaddr>	Enter the host IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create static host name "www.example.com":

```
DGS-3200-10:4# create host_name www.example.com 10.10.10.10
Command: create host_name www.example.com 10.10.10.10

Success.

DGS-3200-10:4#
```

71-6 delete host_name

Purpose

To delete the static or dynamic host name entries of the Switch.

Format

delete host_name [<name 255> | all]

Description

This command is used to delete the static or dynamic host name entries of the Switch.

Parameters

Parameters	Description
<name 255>	Enter the hostname up to 255 characters long.
all	Specify to delete all the hostnames.

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete the static host name entry "www.example.com":

```
DGS-3200-10:4# delete host_name www.example.com
Command: delete host_name www.example.com

Success.

DGS-3200-10:4#
```

71-7 show host_name

Purpose

To display the current host name.

Format

show host_name {static | dynamic}

Description

This command is used to display the current host name.

Parameters

Parameters	Description
static	Specify to display the static host name entries.
dynamic	Specify to display the dynamic host name entries.

Restrictions

None.

Examples

To display the static and dynamic host name entries:

```
DGS-3200-10:4# show host_name
Command: show host_name

Static Host Name Table
Host Name                      IP Address
-----------------------------  ---------------
www.example.com                 10.10.10.10
www.exampla.com                 20.20.20.20

Total Static Entries: 2

Dynamic Host Name Table
Host Name                      IP Address      TTL
-----------------------------  --------------- -----------
www.examplc.com                 30.30.30.30     60 minutes
www.exampld.com                 40.40.40.40     10 minutes

Total Dynamic Entries: 2

DGS-3200-10:4#
```

71-8 enable dns_resolver

Purpose

To enable the DNS Resolver state of the Switch.

Format

enable dns_resolver

Description

This command is used to enable the DNS Resolver state of the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DNS Resolver state to enabled:

```
DGS-3200-10:4# enable dns_resolver
Command: enable dns_resolver

Success.

DGS-3200-10:4#
```

71-9 disable dns_resolver

Purpose

To disable the DNS Resolver state of the Switch.

Format

disable dns_resolver

Description

This command is used to disable the DNS Resolver state of the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DNS Resolver state to disabled:

```
DGS-3200-10:4# admin# disable dns_resolver

Command: disable dns_resolver


Success.


DGS-3200-10:4#
```

72 PPPoE Circuit ID Insertions Command List

config pppoe circuit_id_insertion state [enable | disable]
config pppoe circuit_id_insertion ports <portlist> {state [enable | disable] |circuit_id [mac|ip|udf <string 32>]}
show pppoe circuit_id_insertion
show pppoe circuit_id_insertion ports {<portlist>}

72-1 config pppoe circuit_id_insertion state

Purpose

To enable or disable PPPoE circuit ID insertion function.

Format

config pppoe circuit_id_insertion state [enable | disable]

Description

This command is used to enable or disable PPPoE circuit ID insertion function. When the setting is enabled, the system will insert the circuit ID tag to the received PPPoE discover and request packet if the tag is absent, and remove the circuit ID tag from the received PPPoE offer and session confirmation packet. The insert circuit ID contains the following information: Client MAC address, Device ID and Port number. By default, Switch IP address is used as the device ID to encode the circuit ID option.

Parameters

Parameters	Description
enable	Specify to enable the PPPoE circuit ID insertion on the Switch.
disable	Specify to disable the PPPoE circuit ID insertion on the Switch.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable the PPPoE circuit insertion state:

```
DGS-3200-10:4# config pppoe circuit_id_insertion enable
Command: config pppoe circuit_id_insertion enable

Success.

DGS-3200-10:4#
```

72-2 config pppoe circuit_id_insertion ports

Purpose

To configure port's PPPoE Circuit ID insertion function.

Format

config pppoe circuit_id_insertion ports <portlist> {state [enable | disable] |circuit_id [mac|ip|udf <string 32>]}

Description

This command is used to configure port's PPPoE Circuit ID insertion function. When the port's state and the global state are enabled, the system will insert the Circuit ID TAG to the received PPPoE discovery initiation and request packet if the TAG is absent, and remove the Circuit ID TAG from the received PPPoE offer and session confirmation packet.

Parameters

Parameters	Description
<portlist>	Specify a list of ports to be configured.
state	Specify to enable or disable port's PPPoE circuit ID insertion function. The default setting is enable.
ciuciut_id	Configure the device ID part for encoding of the circuit ID option. **mac** - The MAC address of the Switch will be used to encode the circuit ID option. **ip** - The Switch's IP address will be used to encode the circuit ID option. This is the default. **udf** - A user specified string to be used to encode the circuit ID option. The maximum length is 32.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable port 5 PPPoE circuit ID insertion function:

```
DGS-3200-10:4# config pppoe circuit_id_insertion ports 5 state enable
Command: config pppoe circuit_id_insertion ports 5 state enable

Success.

DGS-3200-10:4#
```

72-3 show pppoe circuit_id_insertion

Purpose

To show PPPoE circuit ID insertion status.

Format

show pppoe circuit_id_insertion

Description

This command is used to display PPPoE circuit ID insertion status.

Parameters

None.

Restrictions

None.

Examples

To display PPPoE circuit ID insertion status:

```
DGS-3200-10:4# show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion


Global PPPoE State: Enabled


DGS-3200-10:4#
```

72-4 show pppoe circuit_id_insertion ports

Purpose

To display Switch's port PPPoE Circuit ID insertion configuration.

Format

show pppoe circuit_id_insertion ports {<portlist>}

Description

This command is used to display Switch's port PPPoE Circuit ID insertion configuration.

Parameters

Parameters	Description
<portlist>	Specify a list of ports to be displayed.

Restrictions

None.

Examples

To display port 2-5 PPPoE circuit ID insertion configuration:

```
DGS-3200-10:4# show pppoe circuit_id_insertion ports 2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port State     Circuit ID
---- --------- -------------------------------------------
2    Disabled  Switch MAC
3    Enabled   Switch IP
4    Disabled  Switch IP
5    Enabled   Switch MAC

DGS-3200-10:4#
```

XI. IPv6

The IPv6 section includes the following chapter: IPv6 NDP and DHCPv6 Relay.

73 IPv6 NDP Command List

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif [<ipif_name 12>|all] [<ipv6addr> | static| dynamic| all]
show ipv6 neighbor_cache ipif [<ipif_name 12>|all] [ipv6address <ipv6addr> | static|dynamic|all]
config ipv6 nd ns ipif <ipif_name 12> retrans_timer <uint 0-4294967295>
show ipv6 nd {ipif <ipif_name 12>}

73-1 delete ipv6 neighbor_cache

Purpose

To add a static neighbor on an IPv6 interface.

Format

create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>

Description

This command is used to add a static neighbor on an IPv6 interface

Parameters

Parameters	Description
ipif_name	The interface's name.
ipv6addr	The address of the neighbor.
macaddr	The MAC address of the neighbor.

Restrictions

Only Administrator-level users can issue this command.

Examples

To create a static neighbor cache entry:

```
DGS-3200-10:4#create ipv6 neighbor_cache ipif System 3ffc::1  00:01:02:03:04:05
Command: create ipv6 neighbor_cache ipif System 3FFC::1 00-01-02-03-04-05

Success.

DGS-3200-10:4#
```

73-2 delete ipv6 neighbor_cache

Purpose

To delete an IPv6 neighbor from the interface neighbor address cache.

Format

delete ipv6 neighbor_cache ipif [<ipif_name 12>|all] [<ipv6addr> | static| dynamic| all]

Description

This command is used to delete a neighbor cache entry or static neighbor cache entries from the address cache or all address cache entries on this IPIF. Both static and dynamic entry can be deleted.

Parameters

Parameters	Description
ipif_name	The IPv6 interface.
ipv6addr	The address of the neighbor.
all	All entries include static and dynamic entries will be deleted.
dynamic	Delete those dynamic entries.
static	Delete the static entry

Restrictions

Only Administrator-level users can issue this command.

Examples

To delete a neighbor cache:

```
DGS-3200-10:4#delete ipv6 neighbor_cache ipif System 3ffc::1
Command: delete ipv6 neighbor_cache ipif System 3FFC::1

Success.

DGS-3200-10:4#
```

73-3 show ipv6 neighbor_cache

Purpose

To display an IPv6 neighbor cache.

Format

show ipv6 neighbor_cache ipif [<ipif_name 12>|all] [ipv6address <ipv6addr> | static|dynamic|all]

Description

This command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all entries, and all static entries..

Parameters

Parameters	Description
<ipif_name 12>	The interface's name.
<ipv6addr>	The address of the entry.
static	Static neighbor cache entry.
dynamic	Dynamic entries.

Restrictions

None.

Examples

To display an IPv6 neighbor cache:

```
DGS-3200-10:4#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                    Link Layer Address  Interface    State
--------------------------  ------------------  -----------  -----
FE80::20B:6AFF:FECF:7EC6    00-0B-6A-CF-7E-C6   System        T

Total Entries: 1

State:
(I) means Incomplete state. (R) means Reachable state.
(S) means Stale state.      (D) means Delay state.
(P) means Probe state.      (T) means Static state.


DGS-3200-10:4#
```

73-4 config ipv6 nd ns

Purpose

To configure neighbor solicitation related arguments.

Format

config ipv6 nd ns ipif <ipif_name 12> retrans_timer <uint 0-4294967295>

Description

This command is used to configure neighbor solicitation related arguments.

Parameters

Parameters	Description
ipif_name	The name of the interface.
ns retrans_timer	Neighbor solicitation's retransmit timer in milliseconds. It has the same value as ra retrans_time in the config ipv6 nd ra command. If we configure one, the other will change too.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure neighbor solicitation related arguments:

```
DGS-3200-10:4#config ipv6 nd ns ipif System retrans_time 400
Command: config ipv6 nd ns ipif System retrans_time 400

Success.

DGS-3200-10:4#
```

73-5 show ipv6 nd

Purpose

To display an interface's information.

Format

show ipv6 nd {ipif <ipif_name 12>}

Description

This command is used to display IPv6 ND related configuration.

Parameters

Parameters	Description
ipif_name	The interface name.

Restrictions

None.

Examples

To display an interface's information:

```
DGS-3200-10:4#show ipv6 nd ipif System
Command: show ipv6 nd ipif System

Interface Name                  : System
NS Retransmit Time              : 0 (ms)

DGS-3200-10:4#
```

74 DHCPv6 Relay Command List

config dhcpv6_relay hop_count <value 1-32>
config dhcpv6_relay [add|delete] ipif <ipif_name 12> <ipv6addr>
config dhcpv6_relay ipif [<ipif_name 12> |all] state [enable | disable]
show dhcpv6_relay {ipif <ipif_name 12>}
enable dhcpv6_relay
disable dhcpv6_relay

74-1 config dhcpv6_relay hop_count

Purpose

To configure the DHCPv6 relay hop count of the switch.

Format

config dhcpv6_relay hop_count <value 1-32>

Description

This command is used to configure the DHCPv6 relay hop count of the switch.

Parameters

Parameters	Description
<value 1-32>	Enter the number of relay agents that have to be relayed in this message. The range is from 1 to 32. The default value is 4.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the maximum hops of a DHCPv6 relay packet that can be transferred to 4:

```
DGS-3200-10:4# config dhcpv6_relay hop_count 4
Command: config dhcpv6_relay hop_count 4


Success.



DGS-3200-10:4#
```

74-2 config dhcpv6_relay

Purpose

To add or delete an IPv6 address which is a destination to forward (relay) DHCPv6 packets.

Format

config dhcpv6_relay [add|delete] ipif <ipif_name 12> <ipv6addr>

Description

The command is used to add or delete an IPv6 address which is a destination to forward (relay) DHCPv6 packets.

Parameters

Parameters	Description
add	Add an IPv6 destination to the DHCPv6 relay table.
delete	Delete an IPv6 destination from the DHCPv6 relay table.
ipif_name	The name of the IP interface in which DHCPv6 relay is to be enabled.
ipv6addr	The DHCPv6 server IP address.

Restrictions

Only Administrator-level users can issue this command.

Examples

To add a DHCPv6 server to the relay table:

```
DGS-3200-10:4# config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E
Command: config dhcpv6_relay add ipif System 2001:DB8:1234:0:218:FEFF:FEFB:CC0E

Success.

DGS-3200-10:4#
```

74-3 config dhcpv6_relay ipif

Purpose

To configure the DHCPv6 relay state of one or all of the specified interfaces.

Format

config dhcpv6_relay ipif [<ipif_name 12> |all] state [enable | disable]

Description

This command is used to configure the DHCPv6 relay state of one or all of the specified interfaces.

Parameters

Parameters	Description
<ipif_name 12>	Specify the name of the IP interface. The value **all** indicates all configured IP interfaces.
state	Enable or disable the DHCPv6 relay state of the interface.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DHCPv6 relay state of the System interface to enable:

```
DGS-3200-10:4# config dhcpv6_relay ipif System state enable
Command: config dhcpv6_relay ipif System state enable

Success.

DGS-3200-10:4#
```

74-4 show dhcpv6_relay

Purpose

To display the current DHCPv6 relay configuration.

Format

show dhcpv6_relay {ipif <ipif_name 12>}

Description

This command will display the current DHCPv6 relay configuration of all interfaces, or if an IP interface name is specified, the DHCPv6 relay configuration for that IP interface.

Parameters

Parameters	Description
ipif	The name of the IP interface that will be displayed in the current DHCPv6 relay configuration. If not specified, all configured DHCPv6 relay interfaces will be displayed.

Restrictions

None.

Examples

To show the DHCPv6 relay configuration of all interfaces:

```
DGS-3200-10:4#show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
------------------------------------------------------------------
IP Interface              : System
DHCPv6 Relay Status       : Enabled
Server Address            :

 Total Entries   : 1



DGS-3200-10:4#
```

To show the DHCPv6 relay configuration of System interface:

```
GS-3200-10:4#show dhcpv6_relay ipif System
Command: show dhcpv6_relay ipif System

DHCPv6 Relay Global State : Disabled
DHCPv6 Hops Count Limit   : 4
------------------------------------------------------------------
IP Interface              : System
DHCPv6 Relay Status       : Enabled
Server Address            :

 Total Entries   : 1



DGS-3200-10:4#
```

74-5 enable dhcpv6_relay

Purpose

To enable the DHCPv6 relay function on the Switch.

Format

enable dhcpv6_relay

Description

This command is used to enable the DHCPv6 relay function on the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DHCPv6 relay global state to enable:

```
DGS-3200-10:4# enable dhcpv6_relay
Command: enable dhcpv6_relay

Success.

DGS-3200-10:4#
```

74-6 disable dhcpv6_relay

Purpose

To disable the DHCPv6 relay function on the Switch.

Format

disable dhcpv6_relay

Description

This command is used to disable the DHCPv6 relay function on the Switch.

Parameters

None.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the DHCPv6 relay global state to disable:

```
DGS-3200-10:4# disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.
```

```
DGS-3200-10:4#
```

XII. ACL

The ACL section includes the following chapter: ACL.

75 ACL Command List

create access_profile profile_id <value 1-200> **[ethernet** **{ vlan | source_mac <macmask 000000000000-ffffffffffff> |** **destination_mac <macmask 000000000000-ffffffffffff> |** **802.1p | ethernet_type }** **| ip** **{ vlan** **source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp |** **[icmp {type | code } | igmp {type } |** **tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask(<hex 0x0-0xffff> |** **flag_mask [all | {urg | ack | psh| rst| syn | fin}] } |** **udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |** **protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}** **| packet_content_mask** **{ offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff>** **offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff>** **offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff>** **offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff> }** **| ipv6** **{class | flowlabel | source_ipv6_mask<ipv6mask> | destination_ipv6_mask <ipv6mask>}]**
delete access_profile [profile_id <value 1-200> | all]
config access_profile profile_id <value 1-200> [add access_id [auto_assign | <value 1-200>] **[ethernet** **{vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |** **destination_mac <macaddr 000000000000-ffffffffffff> | 802.1p <value 0-7> | ethernet_type** **<hex 0x0-0xffff> }** **| ip** **{vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63>** **| [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp** **{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin } |** **udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255>**

{user_define <hex 0x0-0xffffffff>}]}
| packet_content
{offset_chunk_1 <hex 0x0-0xffffffff> | offset_chunk_2 <hex 0x0-0xffffffff> |
offset_chunk_3 <hex 0x0-0xffffffff> | offset_chunk_4 <hex 0x0-0xffffffff>}
| ipv6
{class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> |
destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit { priority <value 0-7>
{replace_priority} | replace_dscp <value 0-63> | rx_rate [no_limit| <value 1-15625>] |
counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete
access_id <value 1-200>]
show access_profile {profile_id <value 1-200>}
config time_range <range_name 32> [hours start_time <time hh:mm:ss> end_time <time hh:mm:ss> weekdays <daylist> |delete]
show time_range
create cpu access_profile profile_id <value 1-5>
[ethernet
{ vlan | source_mac <macmask 000000000000-ffffffffffff> |
destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}
| ip
{ vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> |
dscp | [icmp {type | code} | igmp {type } |
tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> |
flag_mask [all | {urg | ack | psh | rst | syn| fin}] } |
udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
| packet_content_mask
{offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>} | ipv6
{class | flowlabel| source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]
delete cpu access_profile [profile_id <value 1-5> |all]

config cpu access_profile profile_id <value 1-5> **[add access_id <value 1-100>** **[ethernet** **{vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |** **destination_mac <macaddr 000000000000-ffffffffffff> |** **802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }** **| ip** **{vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |** **[icmp {type <value 0-255> | code <value 0-255>} |** **igmp {type <value 0-255>} |** **tcp{src_port <value 0-65535> | dst_port <value 0-65535> |** **urg | ack | psh | rst | syn | fin } |** **udp {src_port <value 0-65535> | dst_port <value 0-65535>} |** **protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}] }** **| packet_content** **{offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |** **offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|** **offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|** **offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|** **offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> }** **| ipv6** **{class <value 0-255> | flowlabel <hex 0x0-0xfffff>|** **source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}]** **port [<portlist> | all] [permit | deny] {time_range <range_name 32>}** **| delete access_id <value 1-100>]**
show cpu access_profile {profile_id <value 1-5>}
enable cpu_interface_filtering
disable cpu_interface_filtering

75-1 create access_profile profile_id

Purpose

To create access list rules.

Format

create access_profile profile_id <value 1-200>
[ethernet
{ vlan | source_mac <macmask 000000000000-ffffffffffff> |
destination_mac <macmask 000000000000-ffffffffffff> |
802.1p | ethernet_type } | ip
{ vlan
source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp |
[icmp {type | code } | igmp {type } |
tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask(<hex 0x0-0xffff> |
flag_mask [all | {urg | ack | psh| rst| syn | fin}] } |
udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
| packet_content_mask
{offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff>
offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff>
offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff>
offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>} | ipv6
{class | flowlabel | source_ipv6_mask<ipv6mask> | destination_ipv6_mask <ipv6mask>}]

Description

This command is used to create access list rules.

Note: Please see the Appendix section entitled “Mitigating ARP Spoofing Attacks Using Packet Content ACL” for a configuration example and further information.

Parameters

Parameters	Description
vlan	Specify a VLAN mask.
source_mac	Specify the source MAC mask.
destination_mac	Specify the destination MAC mask.
802.1p	Specify 802.1p priority tag mask.
ethernet_type	Specify the Ethernet type mask.
vlan	Specify a VLAN mask.
source_ip_mask	Specify an IP source submask.
destination_ip_mask	Specify an IP destination submask.

<table>
<tr><td>dscp</td><td colspan="3">Specify the DSCP mask.</td></tr>
<tr><td>icmp</td><td colspan="3">Specify that the rule applies to icmp traffic.</td></tr>
<tr><td></td><td>type</td><td colspan="2">Specify the ICMP packet type.</td></tr>
<tr><td></td><td>code</td><td colspan="2">Specify the ICMP code.</td></tr>
<tr><td>igmp</td><td colspan="3">Specify that the rule applies to IGMP traffic.</td></tr>
<tr><td></td><td>type</td><td colspan="2">Specify the IGMP packet type</td></tr>
<tr><td>tcp</td><td colspan="3">Specify that the rule applies to TCP traffic.</td></tr>
<tr><td></td><td>src_port_mask</td><td colspan="2">Specify the TCP source port mask.</td></tr>
<tr><td></td><td>dst_port_mask</td><td colspan="2">Specify the TCP destination port mask.</td></tr>
<tr><td></td><td>flag_mask</td><td colspan="2">Specify the TCP flag field mask.</td></tr>
<tr><td>udp</td><td colspan="3">Specify that the rule applies to UDP traffic.</td></tr>
<tr><td></td><td>src_port_mask</td><td colspan="2">Specify the UDP source port mask.</td></tr>
<tr><td></td><td>dst_port_mask</td><td colspan="2">Specify the UDP destination port mask.</td></tr>
<tr><td>protocol_id_mask</td><td colspan="3">Specify the protocol id mask.</td></tr>
<tr><td></td><td>user_define_mask</td><td colspan="2">Specify the L4 part mask.</td></tr>
<tr><td>packet_content_mask</td><td colspan="3">Specify the frame content mask. There are a maximum of four offsets that can be configured. Each offset presents four bytes, the range of a mask of a frame is 32 bytes (eight offsets) in the first eighty bytes of frame.</td></tr>
<tr><td>offset</td><td colspan="3">Specify the mask pattern offset of frame.</td></tr>
<tr><td>offset_chunk_1,
offset_chunk_2,
offset_chunk_3,
offset_chunk_4</td><td colspan="3">Specify the frame content offset and mask. Up to four trunk offset and masks in maximum can be configured. A trunk mask presents 4 bytes. Four offset chunks can be selected out from 32 predefined offset chunks as described below:
<table>
<tr><td>chunk0</td><td>chunk1</td><td>chunk2</td><td>……</td><td>chunk29</td><td>chunk30</td><td>chunk31</td></tr>
<tr><td>B126,
B127,
B0,
B1</td><td>B2,
B3,
B4,
B5</td><td>B6,
B7,
B8,
B9</td><td>……</td><td>B114,
B115,
B116,
B117</td><td>B118,
B119,
B120,
B121</td><td>B122,
B123,
B124,
B125</td></tr>
</table>
Example:
offset_chunk_1 0 0xffffffff will match packet byte offset 126,127,0,1
offset_chunk_1 0 0x0000ffff will match packet byte offset 0,1
Note: Only one packet content mask profile can be created.</td></tr>
<tr><td>class</td><td colspan="3">Specify the IPv6 class mask.</td></tr>
<tr><td>flowlabel</td><td colspan="3">Specify the IPv6 flow label mask.</td></tr>
<tr><td>source_ipv6_mask</td><td colspan="3">Specify the IPv6 source IP mask.</td></tr>
<tr><td>destination_ipv6_mask</td><td colspan="3">Specify the IPv6 destination IP mask.</td></tr>
</table>

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of 200 profiles.

Example

To create access list rules:

```
DGS-3200-10:4#create access_profile profile_id 100 ethernet vlan source_mac FF-F
F-FF-FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type
Command: create access_profile profile_id 100 ethernet vlan source_mac FF-FF-FF-
FF-FF-FF destination_mac 00-00-00-FF-FF-FF 802.1p ethernet_type

Success.

DGS-3200-10:4#

DGS-3200-10:4#create access_profile profile_id 101 ip vlan source_ip_mask 255.25
5.255.255 destination_ip_mask 255.255.255.0 dscp icmp
Command: create access_profile profile_id 101 ip vlan source_ip_mask 255.255.255
.255 destination_ip_mask 255.255.255.0 dscp icmp

Success.

DGS-3200-10:4#
```

75-2 delete access_profile

Purpose

To delete access list rules.

Format

delete access_profile [profile_id <value 1-200> | all]

Description

This command is used to delete access list rules.

Parameters

Parameters	Description
profile_id	Specify the index of access list profile.
all	Specify the whole access list profile to delete.

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of 200 access entries. The **delete access_profile** command can only delete the profile which is created by the ACL module.

Example

To delete access list rules:

```
DGS-3200-10:4#delete access_profile profile_id 10
Command: delete access_profile profile_id 10

Success.

DGS-3200-10:4#
```

75-3 config access_profile

Purpose

To configure access list entries.

Format

config access_profile profile_id <value 1-200> [add access_id [auto_assign | <value 1-200>] [ethernet

{vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> | destination_mac <macaddr 000000000000-ffffffffffff> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }

| ip

{vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> | [icmp {type <value 0-255> | code <value 0-255>} | igmp {type <value 0-255>} | tcp {src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin } | udp {src_port <value 0-65535> | dst_port <value 0-65535>} | protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}]}

| packet_content

{offset_chunk_1 <hex 0x0-0xffffffff> | offset_chunk_2 <hex 0x0-0xffffffff> | offset_chunk_3 <hex 0x0-0xffffffff> | offset_chunk_4 <hex 0x0-0xffffffff>}

| ipv6

{class <value 0-255> | flowlabel <hex 0x0-0xfffff> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}] port [<portlist> | all] [permit { priority <value 0-7> {replace_priority} | replace_dscp <value 0-63> | rx_rate [no_limit| <value 1-15625>] | counter [enable | disable]} | mirror | deny] {time_range <range_name 32>} | delete

access_id <value 1-200>]

Description

This command is used to configure access list entries.

Note: Please see the Appendix section entitled “Mitigating ARP Spoofing Attacks Using Packet Content ACL” for a configuration example and further information.

Parameters

Parameters	Description		
profile_id	Specify the index of the access list profile.		
access_id	Specify the index of the access list entry. The range of this value is 1 to 200.		
	vlan	Specify a VLAN name.	
	source_mac	Specify the source MAC.	
	destination_mac	Specify the destination MAC.	
	802.1p	Specify the value of 802.1p priority tag, the value can be configured between 0 to 7.	
	ethernet_type	Specify the Ethernet type.	
	vlan	Specify a VLAN name.	
	source_ip	Specify an IP source address.	
	destination_ip	Specify an IP destination address.	
	dscp	Specify the value of DSCP, the value can be configured from 0 to 63.	
	icmp	Specify that the rule applies to ICMP traffic.	
		type	Specify the ICMP packet type.
		code	Specify the ICMP packet code.
	igmp	Specify that the rule applies to IGMP traffic.	
		type	Specify the IGMP packet type.
	tcp	**src_port**	Specify that the TCP source port.
		dst_port	Specify the TCP destination port.
		flag	Specify the TCP flag fields .
	udp	**src_port**	Specify the UDP source port.
		dst_port	Specify the UDP destination port.
	protocol_id	Specify the Protocol ID.	
		user_define	Specify the L4 part value.

	offset_chunk_1, offset_chunk_2, offset_chunk_3, offset_chunk_4	Specify the content of the trunk to be monitored
	class	Specify the IPv6 class value.
	flowlabel	Specify the IPv6 flow label value.
	source_ipv6	Specify the IPv6 source IP value.
	destination_ipv6	Specify the IPv6 destination IP value.
permit	Specify the packets that match the access profile are permit by the switch.	
priority	Specify the packets that match the access profile are remap the 802.1p priority tag field by the switch.	
replace_priority	Specify the packets that match the access profile remarking the 802.1p priority tag field by the switch.	
rx_rate	Specify the limitation of the receive data rate.	
replace_dscp	Specify the DSCP of the packets that match the access profile are modified according to the value.	
counter	Specify whether the counter feature will be enabled or disabled. The Counter feature is used to record the number of packets matching the Access Rule. For example if you create an Ethernet ACL that permits the source MAC address of 00-00-00-00-00-01 access to the Switch and a 1000 packets with the source MAC address of 00-00-00-00-00-01 is received by the Switch, the counter values will be 1000, to indicate that the ACL has matched 1000 packets. This is optional. The default is disabled.	
deny	Specify the packets that match the access profile are filtered by the switch.	
time_range	Specify the name of this time range entry.	

Restrictions

Only Administrator-level users can issue this command.

Example

To configure an access list entry:

```
DGS-3200-10:4#config access_profile profile_id 101 add access_id 1 ip vlan defau
lt source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit
Command: config access_profile profile_id 101 add access_id 1 ip vlan default so
urce_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp port 1 permit

Success.
DGS-3200-10:4#
```

75-4 show access_profile

Purpose

To display the current access list table.

Format

show access_profile {profile_id <value 1-200>}

Description

This command is used to display the current access list table.

Parameters

Parameters	Description
profile_id	Specify the index of the access list profile. If no parameters are specified, all access list profile entries will be displayed.

Restrictions

None.

Example

To display the current access list table:

```
DGS-3200-10:4#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:199
Total Used Rule Entries  :1



Access Profile ID: 100                                      Type : Ethernet
================================================================================
Owner       : ACL
MASK Option :
VLAN          Source MAC          Destination MAC   802.1P  Ethernet Type
              FF-FF-FF-FF-FF-FF   00-00-00-FF-FF-FF
-----------   -----------------   ----------------- ------  -------------
================================================================================
Unused Entries: 200
```

```
Access Profile ID: 101                                          Type : IP
================================================================================
Owner       : ACL
MASK Option :
VLAN          Source IP MASK  Dst. IP MASK    DSCP ICMP
              255.255.255.255 255.255.255.0
-----------   --------------- --------------- ---- -----------------

Access ID : 1               Mode: Permit                RX Rate(64Kbps): no_limit
Ports     : 1
-----------   --------------- --------------- ---- -----------------
default       20.2.2.3         10.1.1.0         3
================================================================================
Unused Entries: 199

DGS-3200-10:4#
```

75-5 config time_range

Purpose

To configure the range of time to activate a function on the switch.

Format

config time_range <range_name 32> [hours start_time < hh:mm:ss > end_time< hh:mm:ss > weekdays <daylist> | delete]

Description

This command is used to define a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on SNTP time or configured time. If this time is not available, then the time range will not be met.

Parameters

Parameters	Description
range_name	Specify the name of the time range settings.
start_time	Specify the starting time in a day. (24-hr time) For example, 19:00 means 7PM. 19 is also acceptable. **start_time** must be smaller than end_time.
end_time	Specify the ending time in a day. (24-hr time)

weekdays	Specify the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days. For example, **mon-fri** (Monday to Friday) **sun, mon, fri** (Sunday, Monday and Friday)
delete	Deletes a time range profile. When a time range profile has been associated with ACL entries, the deletion of this time range profile will fail.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the range of time to activate a function on the switch:

```
DGS-3200-10:4#config time_range testdaily hours start_time 12:0:0 end_time 13:0:
0 weekdays mon,fri
Command: config time_range testdaily hours start_time 12:0:0 end_time 13:0:0 wee
kdays mon,fri

Success.

DGS-3200-10:4#
```

75-6 show time_range

Purpose

To display current access list table.

Format

show time_range

Description

This command is used to display current time range settings.

Parameters

None.

Restrictions

None.

Example

To display current time range setting:

```
DGS-3200-10:4#show time_range
Command: show time_range

Time Range Information
------------------------
Range Name    :  testdaily
Weekdays      :  Mon,Fri
Start Time    :  12:00:00
End Time      :  13:00:00

Total Entries :1

DGS-3200-10:4#
```

75-7 create cpu access_profile

Purpose

To create CPU access list rules.

Format

create cpu access_profile profile_id <value 1-5>
[ethernet
{ vlan | source_mac <macmask 000000000000-ffffffffffff> |
destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}
| ip
{ vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> |
dscp | [icmp {type | code} | igmp {type } |
tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> |
flag_mask [all | {urg | ack | psh | rst | syn| fin}] } |
udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} |
protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}
| packet_content_mask
{offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}
| ipv6
{class | flowlabel| source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}]

Description

This command is used to create CPU access list rules.

Parameters

Parameters	Description	
vlan	Specify a VLAN mask.	
source_mac	Specify the source MAC mask.	
destination_mac	Specify the destination MAC mask.	
802.1p	Specify 802.1p priority tag mask.	
ethernet_type	Specify the Ethernet type mask.	
source_ip_mask	Specify an IP source submask.	
destination_ip_mask	Specify an IP destination submask.	
dscp	Specify the DSCP mask.	
icmp	Specify that the rule applies to ICMP traffic.	
	type	Specify the ICMP packet type.
	code	Specify the ICMP code.
igmp	Specify that the rule applies to IGMP traffic.	
	type	Specify the IGMP packet type
tcp	Specify that the rule applies to TCP traffic.	
	src_port_mask	Specify the TCP source port mask.
	dst_port_mask	Specify the TCP destination port mask.
	flag_mask	Specify the TCP flag field mask.
udp	Specify that the rule applies to UDP traffic.	
	src_port_mask	Specify the UDP source port mask.
	dst_port_mask	Specify the UDP destination port mask.
protocol_id_mask	Specify the Protocol ID mask.	
	user_define_mask	Specify the L4 part mask
packet_content_mask	Specify the packet content mask.	
	offset_0-15	Specify the mask for packet bytes 0-15.
	offset_16-31	Specify the mask for packet bytes 16-31.
	offset_32-47	Specify the mask for packet bytes 32-47.
	offset_48-63	Specify the mask for packet bytes 48-63.
	offset_64-79	Specify the mask for packet bytes 64-79.
class	Specify the IPv6 class mask.	
flowlabel	Specify the IPv6 flow label mask.	
source_ipv6_mask	Specify the IPv6 source IP mask.	
destination_ipv6_mask	Specify the IPv6 destination IP mask.	

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of five CPU profiles to be configured.

Example

To create CPU access list rules:

```
DGS-3200-10:4#create cpu access_profile profile_id 1 ethernet vlan
Command: create cpu access_profile profile_id 1 ethernet vlan

Success.

DGS-3200-10:4#create cpu access_profile profile_id 2 ip source_ip_mask 255.255.2
55.255
Command: create cpu access_profile profile_id 2 ip source_ip_mask 255.255.255.25
5

Success.

DGS-3200-10:4#
```

75-8 delete cpu access_profile

Purpose

To delete CPU access list rules.

Format

delete CPU access_profile [profile_id <value 1-5> | all]

Description

This command is used to delete CPU access list rules.

Parameters

Parameters	Description
profile_id	Specify the index of access list profile.
all	Specify the whole access list profile to delete.

Restrictions

Only Administrator-level users can issue this command. The Switch supports a maximum of 500 access entries. This command can only delete the profile which is created by the CPU ACL module.

Example

To delete access list rules:

```
DGS-3200-10:4#delete cpu access_profile profile_id 3
Command: delete cpu access_profile profile_id 3

Success.

DGS-3200-10:4#
```

75-9 config cpu access_profile

Purpose

To configure a CPU access list entry.

Format

config cpu access_profile profile_id <value 1-5>
[add access_id <value 1-100>
[ethernet
{vlan <vlan_name 32> | source_mac <macaddr 000000000000-ffffffffffff> |
destination_mac <macaddr 000000000000-ffffffffffff> |
802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff> }
| ip
{vlan <vlan_name 32> | source_ip <ipaddr> | destination_ip <ipaddr> | dscp <value 0-63> |
[icmp {type <value 0-255> | code <value 0-255>} |
igmp {type <value 0-255>} |
tcp{src_port <value 0-65535> | dst_port <value 0-65535> | urg | ack | psh | rst | syn | fin } |
udp {src_port <value 0-65535> | dst_port <value 0-65535>} |
protocol_id <value 0 - 255> {user_define <hex 0x0-0xffffffff>}] }
| packet_content
{offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |
offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>|
offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> }
| ipv6
{class <value 0-255> | flowlabel <hex 0x0-0xfffff>|
source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>}]
port [<portlist> | all] [permit | deny] {time_range <range_name 32>}

| delete access_id <value 1-100>]

Description

This command is used to configure CPU access list entries.

Parameters

Parameters	Description		
profile_id	Specify the index of CPU access list profile.		
access_id	Specify the index of an access list entry. The range of this value is 1 to 100.		
	vlan	Specify a VLAN name.	
	source_mac	Specify the source MAC.	
	destination_mac	Specify the destination MAC.	
	802.1p	Specify the value of 802.1p priority tag, the value can be configured between 0 and 7.	
	ethernet_type	Specify the Ethernet type.	
	source_ip	Specify an IP source address.	
	destination_ip	Specify an IP destination address.	
	dscp	Specify the value of DSCP, the value can be configured from 0 to 63.	
	icmp	Specify that the rule applies to ICMP traffic.	
		type	Specify the ICMP packet type.
		code	Specify the ICMP packet code.
	igmp	Specify that the rule applies to IGMP traffic.	
		type	Specify the IGMP packet type.
	tcp	**src_port**	Specify the TCP source port.
		dst_port	Specify the TCP destination port.
		flag	Specify the TCP flag fields.
	udp	**src_port**	Specify the UDP source port.
		dst_port	Specify the UDP destination port.
	protocol_id	Specify the Protocol ID.	
		user_define	Specify the L4 part value.
	packet_content	**offset_0-15**	Specify the value for packet bytes 0-15.
		offset_16-31	Specify the value for packet bytes 16-31.
		offset_32-47	Specify the value for packet bytes 32-47.
		offset_48-63	Specify the value for packet bytes 48-63.
		offset_64-79	Specify the value for packet bytes 64-79.
	class	Specify the IPv6 class value.	

	flowlabel	Specify the IPv6 flow label value.
	source_ipv6	Specify the IPv6 source IP value.
	destination_ipv6	Specify the IPv6 destination IP value.
permit	Specify the packets that match the access profile are permitted by the switch.	
deny	Specify the packets that match the access profile are filtered by the switch.	
time_range	Specify the name of this time range entry.	

Restrictions

Only Administrator-level users can issue this command.

Example

To configure access list entry:

```
DGS-3200-10:4#config cpu access_profile profile_id 1 add access_id 1 ethernet vale
an default port 1-3 deny
Command: config cpu access_profile profile_id 1 add access_id 1 ethernet vlan de
fault port 1-3 deny

Success.

DGS-3200-10:4#
```

75-10 show cpu access_profile

Purpose

To display the current CPU access list table.

Format

show cpu access_profile {profile_id <value 1-5>}

Description

This command is used to display the current CPU access list table.

Parameters

Parameters	Description
profile_id	Specify the index of a CPU access list profile. If no parameters are specified, all CPU access list profile entries will be displayed.

Restrictions

None.

Example

To display the current CPU access list table:

```
DGS-3200-10:4#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries:499
Total Used Rule Entries  :1



Access Profile ID: 1                                    Type : Ethernet
================================================================================
MASK Option :
VLAN
-----------

Access ID : 1               Mode: Deny
Ports     : 1-3
-----------
default
================================================================================
Unused Entries: 99



Access Profile ID: 2                                    Type : IP
================================================================================
MASK Option :
Source IP MASK
255.255.255.255
---------------
================================================================================
Unused Entries: 100



DGS-3200-10:4#
```

75-11 enable cpu_interface_filtering

Purpose

To enable CPU interface filtering.

Format

enable cpu_interface_filtering

Description

This command is used to enable CPU interface filtering.

Parameters

None.

Restrictions

None.

Example

To enable CPU interface filtering:

```
DGS-3200-10:4#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3200-10:4#
```

75-12 disable cpu_interface_filtering

Purpose

To disable CPU interface filtering.

Format

disable cpu_interface_filtering

Description

This command is used to disable CPU interface filtering.

Parameters

None.

Restrictions

None.

Example

To disable CPU interface filtering:

```
DGS-3200-10:4#disable cpu_interface_filtering
Command: disable cpu_interface_filtering


Success.


DGS-3200-10:4#
```

XIII. Packet Control

The Packet Control section includes the following chapter: Packet Storm.

76 Packet Storm Command List

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 512-1024000> | countdown [<min 0> | <min 3-30> | disable] |time_interval <sec5-600>}
config traffic control auto_recover_time [<min 0> | <min 1-65535>]
config traffic control log state [enable | disable]
config traffic trap [none|storm_occurred|storm_cleared|both]
show traffic control{ <portlist> }

76-1 config traffic control

Purpose

To configure broadcast/multicast/unicast packet storm control. A software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism. If the traffic rate is too high, this port will be shut down.

Format

config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 512-1024000> | countdown [<min 0> | <min 3-30> | disable] |time_interval <sec5-600>}

Description

This command is used to configure broadcast/multicast/unicast storm control. Broadcast storm control commands provides H/W storm control mechanism only, and these packet storm control commands include H/W and S/W mechanisms to provide shutdown, recovery, and trap notification functions.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to be configured.
all	
broadcast	Enable or disable broadcast storm control.
multicast	Enable or disable multicast storm control.
unicast	Enable or disable unknown unicast packet storm control (only support

	drop action).
action	There are two actions to take for storm control, **shutdown** and **drop**. The former is implemented in S/W, and the latter is implemented in H/W. If a user chooses **shutdown**, he needs to configure **threshold**, **countdown**, and **time_interval** as well.
threshold	The upper threshold at which the specified storm control will turn on. The **<value 512-1024000>** is the number of broadcast/multicast kbit per second received by the switch that will trigger the storm traffic control measure. Must be an unsigned integer.
countdown	**<min 3-30>** - The timer for shutdown mode. If a port enters the shutdown Rx state and this timer runs out, the port will be shutdown forever. The parameter is not applicable if “drop” (mode) is specified for the “action” parameter. **<min 0>** - 0 disables the forever state, meaning that the port will not enter the shutdown forever state. **disable** - Disable the countdown timer. When the action is shutdown and countdown time is disabled, when the switch detects a storm, it will directly shutdown the port. The default value is 0.
time_interval	The sampling interval of received packet counts. The possible value will be 5 to 600 seconds. This parameter is meaningless for dropping packets is selected as action.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure traffic control and state:

```
DGS-3200-10:4#config traffic control 1-10 broadcast enable action shutdown
threshold 512 time_interval 10
Command: config traffic control 1-10 broadcast enable action shutdown threshold 512
time_interval 10

Success.

DGS-3200-10:4#
```

76-2 config traffic control auto_recover_time

Purpose

To configure the traffic auto recover time that allowed for a port to recover from shutdown forever status.

Format

config traffic control auto_recover_time [<min 0> | <min 1-65535>]

Description

This command is used to configure the traffic auto recover time that allowed for a port to recover from shutdown forever status. The time allowed for auto recovery from shutdown for a port. The default value is 0, so no auto recovery is possible; the port remains in shutdown forever mode. This requires manual entry of the CLI command **config ports [<portlist> | all] state enable** to return the port to a forwarding state. The default value is 0, which means disable auto recover mode, shutdown forever.

Parameters

Parameters	Description
<min 0>	Specify the time to be 0 to disable auto recovery function, and the port remains shut down forever.
<min 1-65535>	Enter the automatic recovery time between 1 and 65535 minutes.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the auto recover time to 5 minutes:

```
DGS-3200-10:4# config traffic control auto_recover_time 5
Command: config traffic control auto_recover_time 5

Success.

DGS-3200-10:4#
```

76-3 config traffic control log state

Purpose

To configure the traffic control log state.

Format

config traffic control log state [enable | disable]

Description

This command is used to configure the traffic control log state. When the log state is enabled, traffic control states are logged when a storm occurs and when a storm is cleared. If the log state is disabled, traffic control events are not logged.

The log state is only applicable for shutdown mode. Since shutdown mode only support broadcast and multicast storm control, doesn't support unicast storm control. The log only generate for broadcast and multicast storm control.

Parameters

Parameters	Description
enable	Specify that traffic control state will be logged when a storm occurs.
disable	Specify that the traffic control state will be disabled.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure the traffic log state on the Switch:

```
DGS-3200-10:4# config traffic control log state enable
Command: config traffic control log state enable

Success.

DGS-3200-10:4#
```

76-4 config traffic trap

Purpose

To configure a traffic control trap.

Format

config traffic trap [none|storm_occurred|storm_cleared|both]

Description

This command is used to configure whether storm control notification will be generated or not while traffic storm events are detected by a SW traffic storm control mechanism.

Note: A traffic control trap is active only when the control action is configured as **shutdown**. If the

control action is **drop** there will no traps issue while storm event is detected.

Parameters

Parameters	Description
none	No notification will be generated when storm event is detected or cleared.
storm_occurred	A notification will be generated when a storm event is detected.
storm_cleared	A notification will be generated when a storm event is cleared.
both	A notification will be generated both when a storm event is detected and cleared.

Restrictions

Only Administrator-level users can issue this command.

Examples

To configure a traffic control trap:

```
DGS-3200-10:4#config traffic trap both
Command: config traffic trap both

Success.

DGS-3200-10:4#
```

76-5 show traffic control

Purpose

To display current traffic control settings.

Format

show traffic control{ <portlist> }

Description

This command is used to display current traffic control settings.

Parameters

Parameters	Description
portlist	Specify a range of ports to be shown. If no parameter is specified, the system will display all port packet storm control configurations.

Restrictions

None.

Examples

To display the packet storm control setting:

```
DGS-3200-10:4#show traffic control
Command: show traffic control



Traffic Control Trap              : [None]
Traffic Control Log               : Enabled
Traffic Control Auto Recover Time: 5 Minutes

Port Thres   Broadcast Multicast Unicast  Action   Count    Time     Shutdown
     hold    Storm     Storm     Storm               down     Interval Forever
---- ------ --------- --------- -------- -------- -------- -------- --------
1    512    Enabled   Disabled  Disabled shutdown 0        10
2    512    Enabled   Disabled  Disabled shutdown 0        10
3    512    Enabled   Disabled  Disabled shutdown 0        10
4    512    Enabled   Disabled  Disabled shutdown 0        10
5    512    Enabled   Disabled  Disabled shutdown 0        10
6    512    Enabled   Disabled  Disabled shutdown 0        10
7    512    Enabled   Disabled  Disabled shutdown 0        10
8    512    Enabled   Disabled  Disabled shutdown 0        10
9    512    Enabled   Disabled  Disabled shutdown 0        10
10   512    Enabled   Disabled  Disabled shutdown 0        10

DGS-3200-10:4#
```

XIV. OAM

The OAM section includes the following chapter: Ethernet OAM and DULD.

77 Ethernet OAM Command List

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]} | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]
show ethernet_oam ports {<portlist>} [status |configuration | statistics |event_log {index <value_list>}]
clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

77-1 config ethernet_oam ports

Purpose

To configure Ethernet OAM.

Format

config ethernet_oam ports [<portlist> | all] [mode [active | passive] | state [enable | disable] | link_monitor [error_symbol {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame {threshold <range 0-4294967295> | window <millisecond 1000-60000> | notify_state [enable | disable]} | error_frame_seconds {threshold <range 1-900> | window <millisecond 10000-900000> | notify_state [enable | disable]} | error_frame_period {threshold <range 0-4294967295> | window <number 148810-100000000> | notify_state [enable | disable]}] | critical_link_event [dying_gasp | critical_event] notify_state [enable | disable] | remote_loopback [start | stop] | received_remote_loopback [process | ignore]]

Description

This command is used to configure Ethernet OAM. The parameter to configure port Ethernet OAM mode operates in active or passive mode. The following two actions are allowed by ports in active mode, but disallowed by ports in passive mode: Initiate OAM discovery and start or stop remote loopback. Note: When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started.

The command used to enable or disable port's Ethernet OAM function. The parameter enabling a port's OAM will cause the port to start OAM discovery. If a port's is active, it initiates the discovery. Otherwise it reacts to the discovery received from peer. Disabling a port's OAM will cause the port to send out a dying gasp event to peers and then disconnect the established OAM link.

The link monitoring parameter is used to configure port Ethernet OAM link monitoring error symbols. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer. The Ethernet OAM link monitoring error frames parameter provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.

The link event parameter configures the capability of the Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event. The command is used to configure the client to process or to ignore the received Ethernet OAM remote loopback command. In remote loopback mode, all user traffic will not be processed. Ignoring the received remote loopback command will prevent the port from entering remote loopback mode.

Parameters

Parameters	Description
portlist	Used to specify a range of ports or all ports to be configured.
mode	Specify to operate in either active mode or passive mode The default mode is active.
state	Specify to enable or disable the OAM function. The default state is disabled.
link_monitor	Used to detect and indicate link faults under a variety of conditions.
error_symbol	Used to generate an error symbol period event to notify the remote OAM peer.
threshold	Specify the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated.
window	The range is 1000 to 60000 ms. The default value is 1000ms.
notify_state	Specify to enable or disable the event notification. The default state is enable.
error_frame	Specify the error frame.
threshold	Specify the number of frame errors in the period that is required to be equal to or greater than in order for the event to be generated.

window	The range is 1000 to 60000 ms .the default value is 1000ms.
notify_state	Specify to enable or disable the event notification. The default state is enable.
error_frame_seconds	Specify error fram time.
threshold	Specify the number of error frame seconds in the period is required to be equal to or greater than in order for the event to be generated.
window	Specify the period of error frame seconds summary event. The range is 10000ms-900000ms and the default value is 60000 ms.
notify_state	Specify to enable or disable the event notification. The default state is enable.
error_frame_period	Specify Ethernet OAM link monitoring error frame period.
threshold	Specify the number of error frame seconds in the period that is required to be equal to or greater than in order for the event to be generated.
window	Specify the period of error frame period event. The period is specified by a number of received frames. The range for this setting is 148810 to 100, 000, 000. The default value is 1488100 frames.
notify_state	Specify to enable or disable the event notification. The default state is enable.
critical_link_event	Specify Ethernet OAM critical link event.
dying_gasp	An unrecoverable local failure condition has occurred.
critical_event	An unspecified critical event has occurred.
notify_state	Specify to enable or disable the event notification. The default state is enabled.
remote_loopback	If **start** is specified, it will request the peer to change to the remote loopback mode. If **stop** is specified, it will request the peer to change to the normal operation mode.
received_remote_loopback	Specify whether to process or to ignore the received Ethernet OAM remote loopback command The default method is **ignore**.

Restrictions

Only Administrator-level users can issue this command.

Example

To configure Ethernet OAM on ports 1 to 2 in active mode:

```
DGS-3200-10:4# config ethernet_oam ports 1-2 mode active
Command: config ethernet_oam ports 1-2 mode active

Success.

DGS-3200-10:4#
```

To enable Ethernet OAM on port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DGS-3200-10:4#
```

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 link_monitor error_symbol threshold 2
window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_symbol threshold 2 window
1000 notify_state enable

Success.

DGS-3200-10:4#
```

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 link_monitor error_frame threshold 2
window 1000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2 window
1000 notify_state enable

Success.


DGS-3200-10:4#
```

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 link_monitor error_frame_seconds
threshold 2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_seconds threshold 2
window 10000 notify_state enable

Success.

DGS-3200-10:4#
```

To configure the error frame threshold to10 and period to 1000000 ms for port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 link_monitor error_frame_period
threshold 10 window 1000000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_period threshold 10
window 1000000 notify_state enable

Success.

DGS-3200-10:4#
```

To configure a dying gasp event for port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 critical_link_event dying_gasp
notify_state enable
Command: config ethernet_oam ports 1 critical_link_event dying_gasp notify_state
enable

Success.

DGS-3200-10:4#
```

To start remote loopback on port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.

DGS-3200-10:4#
```

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-3200-10:4# config ethernet_oam ports 1 received_remote_loopback process

Command: config ethernet_oam ports 1 received_remote_loopback process


Success.


DGS-3200-10:4#
```

77-2 show ethernet_oam ports

Purpose

To display Ethernet OAM information.

Format

show ethernet_oam ports {<portlist>} [status |configuration | statistics |event_log {index <value_list>}]

Description

This command is used to display Ethernet OAM information, including status, configuration, statistics, and event log, on specified ports.

The status information includes:

(1) OAM administration status: enabled or disabled.

(2) OAM operation status. It maybe the below value:

- Disable: OAM is disabled on this port.
- LinkFault: The link has detected a fault and is transmitting OAMPDUs with a link fault indication.
- PassiveWait: The port is passive and is waiting to see if the peer device is OAM capable.
- ActiveSendLocal: The port is active and is sending local information.
- SendLocalAndRemote: The local port has discovered the peer but has not yet accepted or rejected the configuration of the peer.
- SendLocalAndRemoteOk: The local device agrees the OAM peer entity.
- PeeringLocallyRejected: The local OAM entity rejects the remote peer OAM entity.
- PeeringRemotelyRejected: The remote OAM entity rejects the local device.
- Operational: The local OAM entity learns that both it and the remote OAM entity have accepted the peering.
- NonOperHalfDuplex: Since Ethernet OAM functions are not designed to work completely over half-duplex port. This value indicates Ethernet OAM is enabled but the port is in half-duplex operation.

(3) OAM mode: passive or active.

(4) Maximum OAMPDU size: The largest OAMPDU that the OAM entity supports. OAM entities exchange maximum OAMPDU sizes and negotiate to use the smaller of the two maximum OAMPDU sizes between the peers.

(5) OAM configuration revision: The configuration revision of the OAM entity as reflected in the latest OAMPDU sent by the OAM entity. The config revision is used by OAM entities to indicate that configuration changes have occurred, which might require the peer OAM entity to re-evaluate whether OAM peering is allowed.

(6) OAM mode change.

(7) OAM Functions Supported: The OAM functions supported on this port. These functions include:

- Unidirectional: It indicates that the OAM entity supports the transmission of OAMPDUs on links that are operating in unidirectional mode (traffic flowing in one direction only).
- Loopback: It indicates that the OAM entity can initiate and respond to loopback commands.
- Link Monitoring: It indicates that the OAM entity can send and receive Event Notification OAMPDUs.
- Variable: It indicates that the OAM entity can send and receive variable requests to monitor the attribute value as described in the IEEE 802.3 Clause 30 MIB.

The event log displays Ethernet OAM event log information. The switch can buffer 1000 event logs. The event log is different from sys-log as it provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog.

Parameters

Parameters	Description
<portlist>	Specify the range of ports to display.
status	Specify to display the Ethernet OAM status.
configuration	Specify to display the Ethernet OAM configuration.
statistics	Specify to display Ethernet OAM statistics.
event_log	Specify to display the Ethernet OAM event log information.
index	Specify an index range to display.

Restrictions

None.

Example

To display Ethernet OAM statistics information for port 1:

```
DGS-3200-10:4# show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
---------------------------------------------------------------
Information OAMPDU TX                : 0
Information OAMPDU RX                : 0
Unique Event Notification OAMPDU TX   : 0
Unique Event Notification OAMPDU RX   : 0
Duplicate Event Notification OAMPDU TX: 0
Duplicate Event Notification OAMPDU RX: 0
Loopback Control OAMPDU TX            : 0
Loopback Control OAMPDU RX            : 0
Variable Request OAMPDU TX            : 0
Variable Request OAMPDU RX            : 0
Variable Response OAMPDU TX           : 0
Variable Response OAMPDU RX           : 0
Organization Specific OAMPDUs TX      : 0
Organization Specific OAMPDUs RX      : 0
Unsupported OAMPDU TX                 : 0
Unsupported OAMPDU RX                 : 0
Frames Lost Due To OAM                : 0

DGS-3200-10:4#
```

77-3 clear ethernet_oam ports

Purpose

To clear Ethernet OAM information.

Format

clear ethernet_oam ports [<portlist> | all] [event_log | statistics]

Description

This command is used to clear Ethernet OAM information.

Parameters

Parameters	Description
<portlist>	Specify a range of Ethernet OAM ports to be cleared.
all	Specify to clear all Ethernet OAM ports.

event_log	Specify to clear Ethernet OAM event log information.
statistics	Specify to clear Ethernet OAM statistics.

Restrictions

Only Administrator-level users can issue this command.

Example

To clear port 1 OAM statistics:

```
DGS-3200-10:4#clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DGS-3200-10:4#
```

To clear port 1 OAM events:

```
DGS-3200-10:4# admin#clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DGS-3200-10:4#
```

78 D-Link Unidirectional Link Detection (DULD) Command List

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}
show duld ports {<portlist>}

78-1 config duld ports

Purpose

To configure unidirectional link detection on ports.

Format

config duld ports [<portlist> | all] {state [enable | disable] | mode [shutdown | normal] | discovery_time <sec 5-65535>}

Description

The command is used to configure unidirectional link detection on ports. Unidirectional link detection provides discovery mechanism based on 802.3ah to discovery its neighbor. If the OAM discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the link status.

Parameters

Parameters	Description
portlist	Specify a range of ports.
state	Specify these ports unidirectional link detection status. The default state is disabled.
mode	**shutdown** - if any unidirectional link is detected, disable the port and log an event. **normal** - only log an event when a unidirectional link is detected.
discovery_time	Specify these ports neighbor discovery time. If OAM discovery cannot complete in the discovery time, the unidirectional link detection will start. The default discovery time is 5 seconds.

Restrictions

Only Administrator-level users can issue this command.

Examples

To enable unidirectional link detection on port 1:

```
DGS-3200-10:4# config duld ports 1 state enable
Commands: config duld ports 1 state enable

Success.

DGS-3200-10:4#
```

78-1 show duld

Purpose

To show unidirectional link detection information.

Format

show duld ports {<portlist>}

Description

This command is used to show unidirectional link detection information.

Parameters

Parameters	Description
<portlist>	Specify a range of ports to display. If not specified, all ports will be displayed.

Restrictions

None.

Examples

To show ports 1-4 unidirectional link detection information:

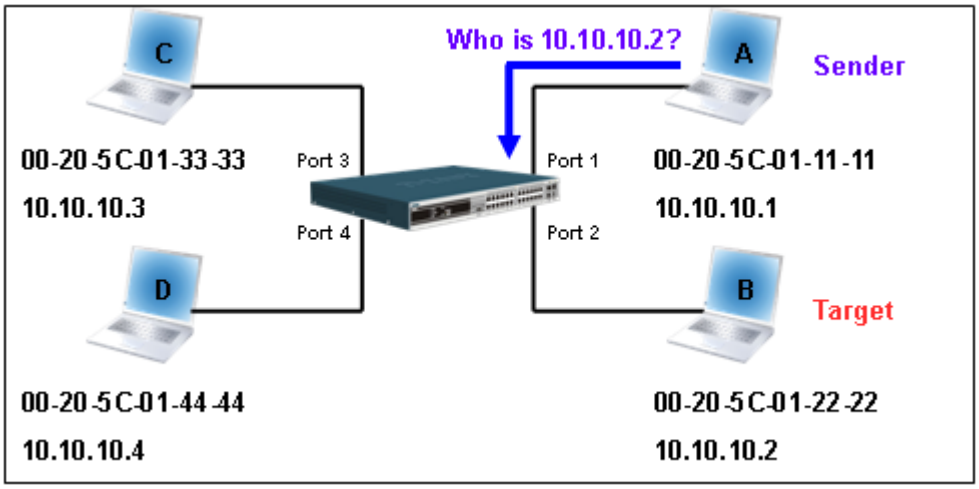
```
DGS-3200-10:4#show duld ports 1-4
Commands: show duld ports 1-4

port  Admin State  Oper Status  Mode      Link Status    Discovery Time(Sec)
----- -----------  -----------  --------  -------------  -------------------
1     Enabled      Enabled      Shutdown  Bidirectional  5
2     Enabled      Enabled      Normal    RX Fault       5
3     Enabled      Enabled      Normal    TX Fault       5
4     Disabled     Disabled     Normal    Unknown        5
5     Enabled      Enabled      Normal    Link Down      5

DGS-3200-10:4#
```

Appendix A - Mitigating ARP Spoofing Attacks Using Packet Content ACL

How Address Resolution Protocol works

In the process of ARP, PC A will first issue an ARP request to query PC B's MAC address. The network structure is shown in Figure 1.

Figure 1



In the meantime, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in the ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00," while PC B's IP address will be written into the "Target Protocol Address," shown in Table 1.

Table 1. ARP Payload

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP request	00-20-5C-01-11-11	10.10.10.1	00-00-00-00-00-00	10.10.10.2

The ARP request will be encapsulated into an Ethernet frame and sent out. As can be seen in Table 2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via broadcast, the "Destination address" is in a format of Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Table 2. Ethernet Frame Format

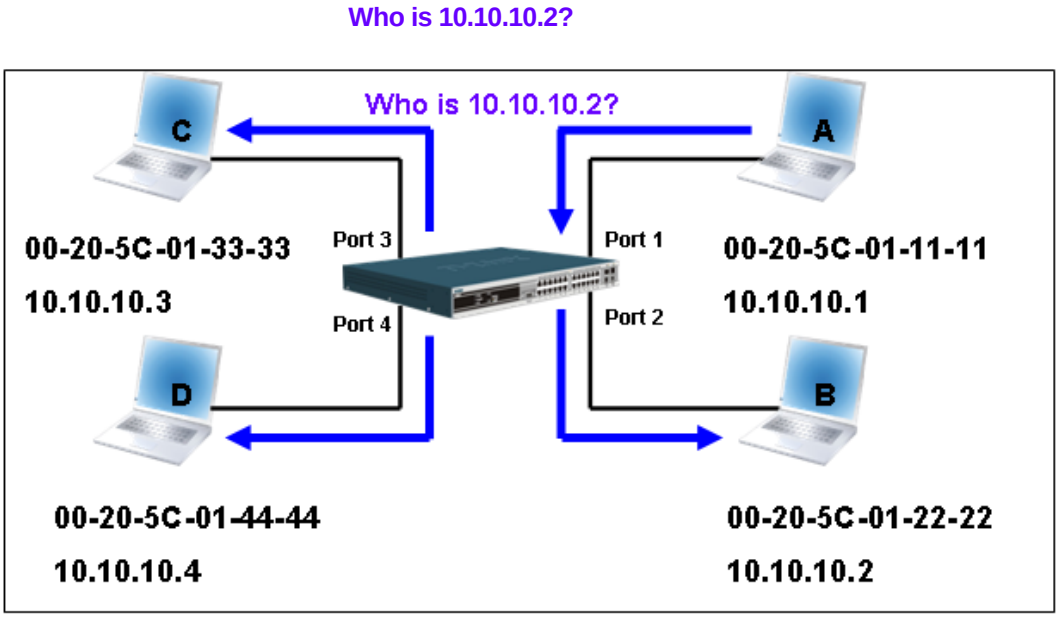
Destination Address	Source Address	Ether-Type	ARP	FCS
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11			

When the switch receives the frame, it will check the “Source Address” in the Ethernet frame’s header. If the address is not in its Forwarding Table, the switch will learn PC A’s MAC and the associated port into its Forwarding Table.

Port1	00-20-5C-01-11-11

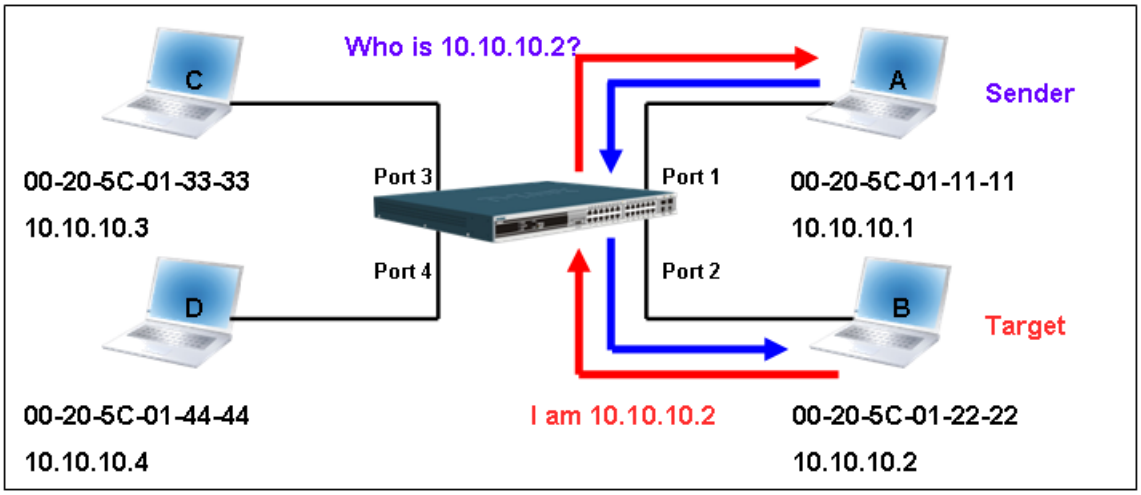
In addition, when the switch receives the broadcasted ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure 2).

Figure 2



When the switch floods the frame of ARP request to the network, all PCs will receive and examine the frame but only PC B will reply the query as the destination IP matched (see Figure 3).

Figure 3



When PC B replies to the ARP request, its MAC address will be written into "Target H/W Address" in the ARP payload shown in Table 3. The ARP reply will be then encapsulated into an Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

Table 3. ARP Payload

H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
				ARP reply	*00-20-5C-01-11-11*	*10.10.10.1*	*00-20-5C-01-22-22*	*10.10.10.2*

When PC B replies to the query, the "Destination Address" in the Ethernet frame will be changed to PC A's MAC address. The "Source Address" will be changed to PC B's MAC address (see Table 4).

Table 4. Ethernet Frame Format

Destination Address	Source Address	Ether-Type	ARP	FCS
00-20-5C-01-11-11	*00-20-5C-01-22-22*			

The switch will also examine the "Source Address" of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B's MAC and update its Forwarding Table.

Forwarding Table

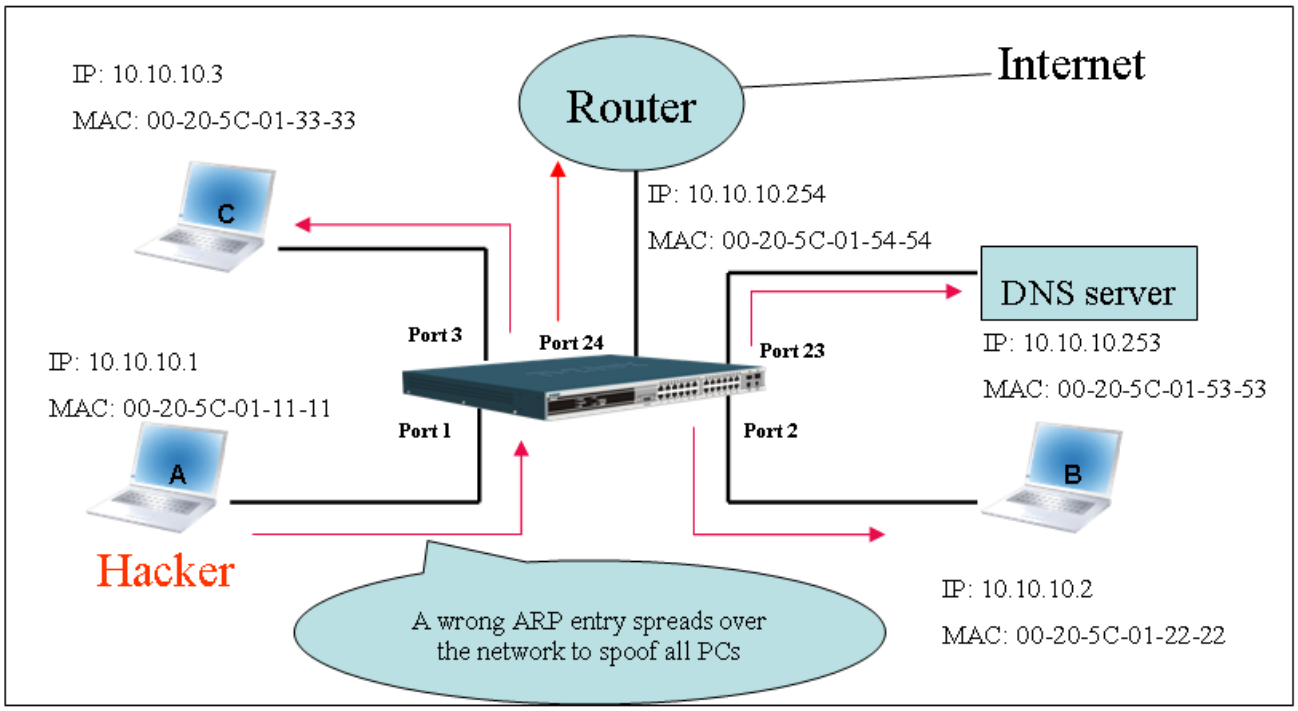
Port1	00-20-5C-01-11-11
Port2	00-20-5C-01-22-22

How ARP Spoofing Attacks a Network

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service – DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure 4 shows a hacker within a LAN to initiate ARP spoofing attack.

Figure 4



In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address itself. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address itself. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in the following table.

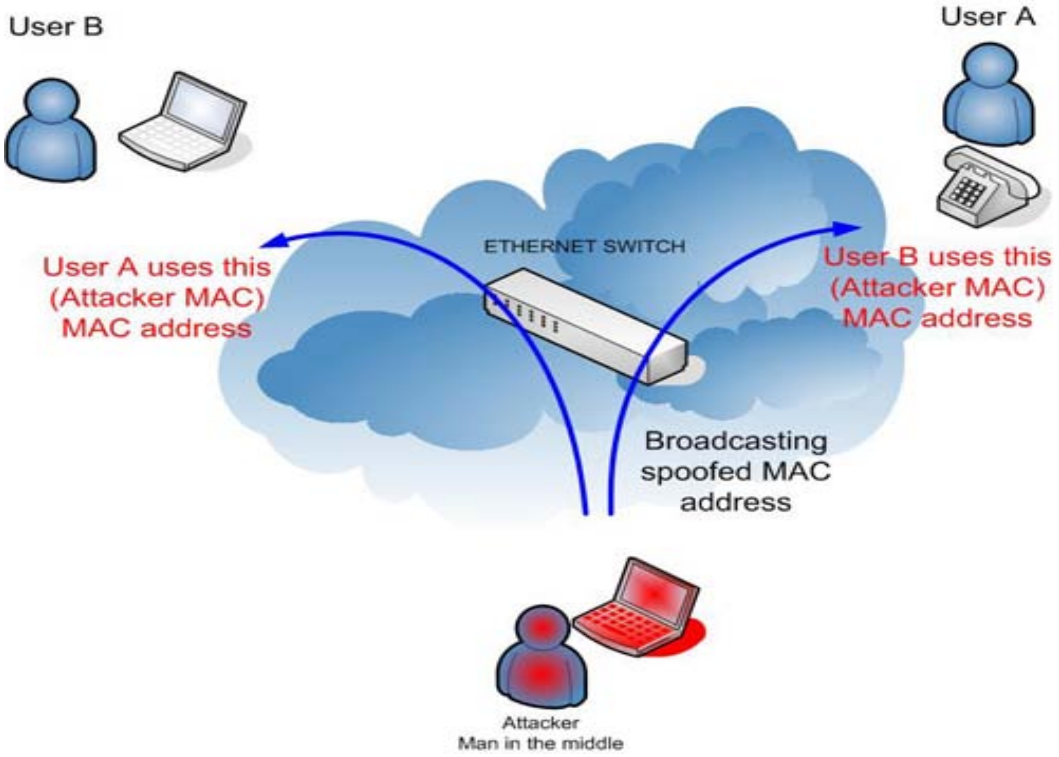
Table 5

Ethernet Header			Gratuitous ARP								
Destination Address	**Source Address**	**Ethernet Type**	**H/W Type**	**Protocol Type**	**H/W Address Length**	**Protocol Address Length**	**Operation**	**Sender H/W Address**	**Sender Protocol Address**	**Target H/W Address**	**Target Protocol Address**
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	0806					ARP relay	***00-20-5C-01-11-11***	***10.10.10.254***	***00-20-5C-01-11-11***	***10.10.10.254***

A common DoS attack today can be done by associating a nonexistent or any specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim PC that it is a router and cheats the router that it is the victim. As can be seen in Figure 5 all traffic will be then sniffed by the hacker but the users will not discover.

Figure 5

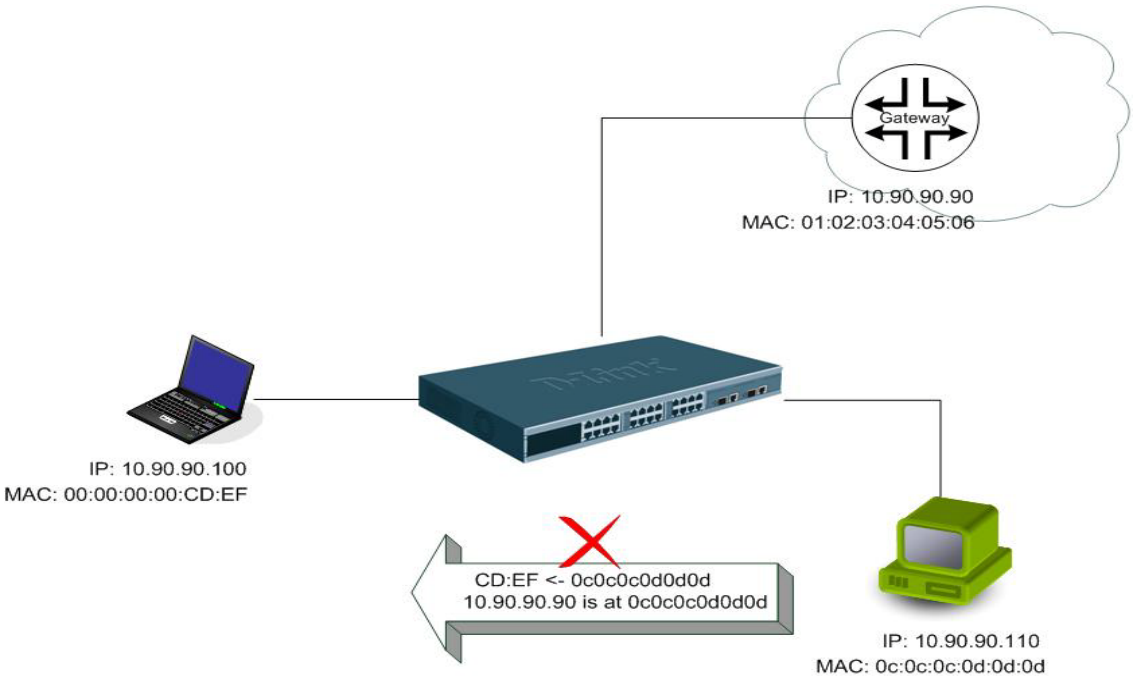


Prevent ARP Spoofing via Packet Content ACL

D-Link managed switches can effectively mitigate common DoS attacks caused by ARP spoofing via a unique Package Content ACL.

For the reason that basic ACL can only filter ARP packets based on packet type, VLAN ID, Source, and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here via using Packet Content ACL to block the invalid ARP packets which contain faked gateway's MAC and IP binding.

Example topology



Configuration

The configuration logic is as follows:

1. Only if the ARP matches Source MAC address in Ethernet, Sender MAC address and Sender IP address in ARP protocol can pass through the switch. (In this example, it is gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL enables users to inspect any offset_chunk. An offset_chunk is a 4-byte block in a HEX format which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of four offset_chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset_chunks can be applied to each profile and a switch. Therefore, a careful consideration is needed for planning and configuration of the valuable offset_chunks.

In Table 6, you will notice that the Offset_Chunk0 starts from the 127th byte and ends at the 128th byte. It also can be found that the offset_chunk is scratched from 1 but not zero.

Table 6. Chunk and Packet Offset

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk30	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

The following table indicates a completed ARP packet contained in Ethernet frame which is the pattern for the calculation of packet offset.

Table 7. A Completed ARP Packet Contained in an Ethernet Frame

Ethernet Header | **ARP**

Destination Address	Source Address	Ethernet Type	H/W Type	Protocol Type	H/W Address Length	Protocol Address Length	Operation	Sender H/W Address	Sender Protocol Address	Target H/W Address	Target Protocol Address
(6-byte)	(6-byte) 01 02 03 04 05 06	(2-byte) 0806	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte) 0a5a5a5a (10.90.90.90)	(6-byte)	(4-byte)

	Command	Description
Step1	create access_profile profile_id 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit	- Configure access profile 1 - Only if the gateway's ARP packet that contains the correct Source MAC in Ethernet frame can pass through the switch.
Step3	create access_profile profile_id 2 profile_name 2 packet_content_mask offset_chunk_1 3 0x0000FFFF Ethernet Type(2-byte) offset_chunk_2 7 0x0000FFFF Sdr IP(First 2-byte) offset_chunk_3 8 0xFFFF0000 Sdr IP(Last 2-byte)	- Create access profile 2 - The first Chunk starts from Chunk 3: mask for Ethernet Type (Blue in Table 6: 13th & 14th bytes) - The second Chunk starts from Chunk 7: mask for Sender IP (First 2-byte) in ARP packet (Green in Table-6: 29th & 30th bytes) - The third Chunk starts from Chunk 8: mask for Sender IP (Last 2-byte) in ARP packet (Brown in Table-6: 31st & 32nd bytes)
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 Ethernet Type(2-byte): ARP offset_chunk_2 0x00000A5A Sdr IP(First 2-byte): 10.90 offset_chunk_3 0x5A5A0000 Sdr IP(Last 2-byte): 90.90 port 1-12 deny	- Configure access profile 2 - The rest the ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step5	Save	- Save config

Appendix B - Password Recovery Procedure

This chapter describes the procedure for resetting passwords on D-Link Switches. 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 get forgotten or destroyed, so network administrators need to reset these passwords. This chapter explains how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. 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.

2. Power on the Switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the “Password Recovery Mode.” Once the Switch enters the “Password Recovery Mode,” all ports on the Switch will be disabled.

```
Boot Procedure                                                    V1.00.B006
--------------------------------------------------------------------------------

  Power On Self Test ....................................  100%

  MAC Address   : 00-19-5B-EC-32-15
  H/W Version   : A2

  Please wait, loading V1.50.B008 Runtime image.............  00 %

The switch is now entering Password Recovery Mode:_
```

```
The switch is currently in Password Recovery Mode.
>
```

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

Command	Parameters
reset config {force_agree}	This command resets the whole configuration back to the default values.
reboot {force_agree}	This command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	The **reset** account command deletes all the previously created accounts.
reset password {<username>}	The **reset password** command resets the password of the specified user. If a username is not specified, the passwords of all users will be reset.
show account	The **show account** command displays all previously created accounts.

Appendix C - System Log Entries

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

Category	Event Description	Log Information	Severity	Remark
System	System started up	System started up	Critical	
	Configuration saved to flash	Configuration saved to flash by console(Username: <username>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	System log saved to flash	System log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console"and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	Configuration and log saved to flash	Configuration and log saved to flash by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, there will no IP and MAC information for logging.
	Left side fan failed	Left side fan <fanID> failed	Critical	For DGS3200-16 and DGS3200-24 only
	Left side fan recovered	Left side fan <fanID> recovered	Critical	For DGS3200-16 and DGS3200-24 only
	Internal Power failed	Internal Power failed	Critical	For DGS3200-24 only
	Internal Power is recovered	Internal Power is recovered	Critical	For DGS3200-24 only
	Redundant Power failed	Redundant Power failed	Critical	For DGS3200-24 only
	Redundant Power is working	Redundant Power is working	Critical	For DGS3200-24 only
Up/Down-load	Firmware upgraded successfully by	Firmware upgraded successfully by	Informational	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR

	console	console(Username: <username>, IP: <ipaddr>)		shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgrade was unsuccessful by console	Firmware upgrade was unsuccessful by console! (Username: <username>, IP: <ipaddr>)	Warning	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully downloaded by console	Configuration successfully downloaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful by console	Configuration download was unsuccessful by console! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully uploaded by console	Configuration successfully uploaded by console (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload was unsuccessful by console	Configuration upload was unsuccessful by console! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message successfully uploaded by console	Log message successfully uploaded by console (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful	Log message upload by console was	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR

	by console	unsuccessful! (Username: <username>, IP: <ipaddr>)		shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgraded successfully by web	Firmware upgraded successfully by Web(Username: <username>, IP: <ipaddr>)	Informational	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgrade was unsuccessful by web	Firmware upgrade was unsuccessful by Web! (Username: <username>, IP: <ipaddr>)	Warning	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully downloaded by web	Configuration successfully downloaded by Web (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful by web	Configuration download by Web was unsuccessful by Web! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully uploaded by web	Configuration successfully uploaded by web (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload was unsuccessful by web	Configuration upload was unsuccessful by Web! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging

	Log message successfully uploaded by web	Log message successfully uploaded by web (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful by web	Log message upload was unsuccessful by Web! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgraded successfully by telnet	Firmware upgraded successfully Telnet (Username: <username>, IP: <ipaddr>)	Informational	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgrade was unsuccessful by telnet	Firmware upgrade was unsuccessful by Telnet ! (Username: <username>, IP: <ipaddr>)	Warning	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully downloaded by telnet	Configuration successfully downloaded by Telnet (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful by telnet	Configuration download was unsuccessful by Telnet! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully uploaded by telnet	Configuration successfully uploaded by Telnet (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload	Configuration upload	Warning	"by console" and "IP": <ipaddr>,

	was unsuccessful by telnet	was unsuccessful by Telnet! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)		MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message successfully uploaded by telnet	Log message successfully uploaded by Telnet (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful by telnet	Log message upload was unsuccessful by Telnet! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgraded successfully by snmp	Firmware upgraded successfully SNMP (Username: <username>, IP: <ipaddr>)	Informational	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Firmware upgrade was unsuccessful by snmp	Firmware upgrade was unsuccessful by SNMP ! (Username: <username>, IP: <ipaddr>)	Warning	“by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully downloaded by snmp	Configuration successfully downloaded by SNMP(Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration download was unsuccessful by snmp	Configuration download was unsuccessful by SNMP! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration successfully	Configuration successfully uploaded	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR

	uploaded by snmp	by SNMP (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)		shown in log string, which means if user login by console, will no IP and MAC information for logging
	Configuration upload was unsuccessful by snmp	Configuration upload was unsuccessful by SNMP! (Username: <username>, IP: <ipaddr>, MAC: <macaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message successfully uploaded by snmp	Log message successfully uploaded by SNMP (Username: <username>, IP: <ipaddr>)	Informational	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
	Log message upload was unsuccessful by snmp	Log message upload was unsuccessful by SNMP! (Username: <username>, IP: <ipaddr>)	Warning	"by console" and "IP": <ipaddr>, MAC: <macaddr>" are XOR shown in log string, which means if user login by console, will no IP and MAC information for logging
Interface	Port link up	Port <portNum> link up, <link state>	Informational	link state, for ex: , 100Mbps FULL duplex
	Port link down	Port <portNum> link down	Informational	
	Link aggregation Group linkUp/linkDown	Link aggregation Group %d (Interface: %d) link up/Link aggregation Group %d (Interface: %d) link down	Information	
Console	Successful login through Console	Successful login through Console (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console	Login failed through Console (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Logout through Console	Logout through Console (Username:	Informational	There are no IP and MAC if login by console.

		<username>)		
	Console session timed out	Console session timed out (Username: <username>)	Informational	There are no IP and MAC if login by console.
Web	Successful login through Web	Successful login through Web (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Web	Login failed through Web (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Web	Logout through Web (Username: <username>, IP: <ipaddr>)	Informational	
	Successful login through Web (SSL)	Successful login through Web (SSL) (Username: <username>, IP: <ipaddr>)	Informational	
	Login failed through Web (SSL)	Login failed through Web (SSL) (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Web (SSL)	Logout through Web (SSL) (Username: <username>, IP: <ipaddr>)	Informational	
	Web (SSL) session timed out	Web (SSL) session timed out (Username: <username>, IP: <ipaddr>)	Informational	
Telnet	Successful login through Telnet	Successful login through Telnet (Username: <username>, IP:	Informational	

		<ipaddr>)		
	Login failed through Telnet	Login failed through Telnet (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through Telnet	Logout through Telnet (Username: <username>, IP: <ipaddr>)	Informational	
	Telnet session timed out	Telnet session timed out (Username: <username>, IP: <ipaddr>)	Informational	
SNMP	SNMP request received with invalid community string	SNMP request received from <ipAddress> with invalid community string!	Informational	
STP	Topology changed	Topology changed (Instance: <InstanceID> port:<portNum>)]	Informational	Detected Topology changed port
	New Root selected	[CIST | MIST Regional] New root selected [([Instance: <InstanceID>] Root bridge MAC: <macaddr> Priority :<value>)]	Informational	root bridge MAC address and priority at the instance
	Spanning Tree Protocol is enabled	Spanning Tree Protocol is enabled	Informational	
	Spanning Tree Protocol is disabled	Spanning Tree Protocol is disabled	Informational	
DoS	Spoofing attack enhance	Possible spoofing attack from IP: <ipAddress> MAC: <macAddress> port: <portNum>	Critical	
SSH	Successful login	Successful login	Informational	

	through SSH	through SSH (Username: <username>, IP: <ipaddr>)		
	Login failed through SSH	Login failed through SSH (Username: <username>, IP: <ipaddr>)	Warning	
	Logout through SSH	Logout through SSH (Username: <username>, IP: <ipaddr>)	Informational	
	SSH session timed out	SSH session timed out (Username: <username>, IP: <ipaddr>)	Informational	
	SSH server is enabled	SSH server is enabled	Informational	
	SSH server is disabled	SSH server is disabled	Informational	
AAA	Authentication Policy is enabled	Authentication Policy is enabled (Module: AAA)	Informational	
	Authentication Policy is disabled	Authentication Policy is disabled (Module: AAA)	Informational	
	Successful login through Console authenticated by AAA local method	Successful login through Console authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Console authenticated by AAA local method	Login failed through Console authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web authenticated by	Successful login through Web from <userIP> authenticated	Informational	

	AAA local method	by AAA local method (Username: <username>)		
	Login failed through Web authenticated by AAA local method	Login failed failed through Web from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Web (SSL) authenticated by AAA local method	Successful login through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Web (SSL) authenticated by AAA local method	Login failed through Web (SSL) from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA local method	Successful login through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Informational	
	Login failed through Telnet authenticated by AAA local method	Login failed through Telnet from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA local method	Successful login through SSH from <userIP> authenticated by AAA local method	Informational	

		(Username: <username>)		
	Login failed through SSH authenticated by AAA local method	Login failed through SSH from <userIP> authenticated by AAA local method (Username: <username>)	Warning	
	Successful login through Console authenticated by AAA none method	Successful login through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web authenticated by AAA none method	Successful login through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Web (SSL) authenticated by AAA none method	Successful login through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through Telnet authenticated by AAA none method	Successful login through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful login through SSH authenticated by AAA none method	Successful login through SSH from <userIP> authenticated by AAA none method (Username:	Informational	

		<username>)		
	Successful login through Console authenticated by AAA server	Successful login through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	There are no IP and MAC if login by console.
	Login failed through Console authenticated by AAA server	Login failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	There are no IP and MAC if login by console.
	Login failed through Console due to AAA server timeout or improper configuration	Login failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Web authenticated by AAA server	Successful login through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Web authenticated by AAA server	Login failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web due to AAA server timeout or improper configuration	Login failed through Web from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login	Successful login	Informational	

	through Web (SSL) authenticated by AAA server	through Web(SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)		
	Login failed through Web (SSL) authenticated by AAA server	Login failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Login failed through Web (SSL) due to AAA server timeout or improper configuration	Login failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful login through Telnet authenticated by AAA server	Successful login through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Login failed through Telnet authenticated by AAA server	Login failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Successful login through SSH authenticated by AAA server	Successful login through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Successful Enable Admin through	Successful Enable Admin through Console	Informational	

	Console authenticated by AAA local_enable method	authenticated by AAA local_enable method (Username: <username>)		
	Enable Admin failed through Console authenticated by AAA local_enable method	Enable Admin failed through Console authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA local_enable method	Successful Enable Admin through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA local_enable method	Enable Admin failed through Web from <userIP> authenticated by AAA local_enable method (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA local_enable method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Successful Enable Admin through SSH authenticated by AAA local_enable method	Successful Enable Admin through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)	Informational	
	Enable Admin failed	Enable Admin failed	Warning	

	through SSH authenticated by AAA local_enable method	through SSH from <userIP> authenticated by AAA local_enable method (Username: <username>)		
	Successful Enable Admin through Console authenticated by AAA none method	Successful Enable Admin through Console authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web authenticated by AAA none method	Successful Enable Admin through Web from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Web (SSL) authenticated by AAA none method	Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through Telnet authenticated by AAA none method	Successful Enable Admin through Telnet from <userIP> authenticated by AAA none method (Username: <username>)	Informational	
	Successful Enable Admin through SSH authenticated by AAA none method	Successful Enable Admin through SSH from <userIP> authenticated by AAA none method (Username:	Informational	

		<username>)		
	Successful Enable Admin through Console authenticated by AAA server	Successful Enable Admin through Console authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Console authenticated by AAA server	Enable Admin failed through Console authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Console due to AAA server timeout or improper configuration	Enable Admin failed through Console due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Web authenticated by AAA server	Successful Enable Admin through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Web authenticated by AAA server	Enable Admin failed through Web from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web due to AAA server timeout or improper configuration	Enable Admin failed through Web from <userIP> due to AAA server timeout or improper configuration (Username:	Warning	

		<username>)		
	Successful Enable Admin through Web (SSL) authenticated by AAA server	Successful Enable Admin through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Web (SSL) authenticated by AAA server	Enable Admin failed through Web (SSL) from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Web (SSL) due to AAA server timeout or improper configuration	Enable Admin failed through Web (SSL) from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	Successful Enable Admin through Telnet authenticated by AAA server	Successful Enable Admin through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through Telnet authenticated by AAA server	Enable Admin failed through Telnet from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through Telnet due to AAA server timeout	Enable Admin failed through Telnet from <userIP> due to AAA	Warning	

	or improper configuration	server timeout or improper configuration (Username: <username>)		
	Successful Enable Admin through SSH authenticated by AAA server	Successful Enable Admin through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Informational	
	Enable Admin failed through SSH authenticated by AAA server	Enable Admin failed through SSH from <userIP> authenticated by AAA server <serverIP> (Username: <username>)	Warning	
	Enable Admin failed through SSH due to AAA server timeout or improper configuration	Enable Admin failed through SSH from <userIP> due to AAA server timeout or improper configuration (Username: <username>)	Warning	
	AAA server timed out	AAA server <serverIP> (Protocol: <protocol>) connection failed	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA server ACK error	AAA server <serverIP> (Protocol: <protocol>) response is wrong	Warning	<protocol> is one of TACACS, XTACACS, TACACS+, RADIUS
	AAA does not support this functionality	AAA doesn't support this functionality	Informational	
IP-MAC-PORT Binding	Unauthenticated IP address and discard by IP MAC port binding	Unauthenticated IP-MAC address and discarded by IP MAC port binding (IP: < ipaddr > | < ipv6addr >,	Warning	

		MAC: <macaddr>, Port <portNum>)		
	Dynamic IMPB entry is conflict with static FDB	Dynamic IMPB entry is conflict with static FDB (IP: < ipaddr > | < ipv6addr >, MAC: <macaddr>, Port <portNum>)	Warning	
	Dynamic IMPB entry is conflict with static ARP	Dynamic IMPB entry is conflict with static ARP (IP: <ipaddr>, MAC: <macaddr>, Port <portNum>)	Warning	
	Dynamic IMPB entry is conflict with static IMPB	Dynamic IMPB entry is conflict with staticIIMPB (IP: < ipaddr > | < ipv6addr >, MAC: <macaddr>, Port <portNum>)	Warning	
	Creating IMPB entry Failed due to no ACL rule available	Creating IMPB entry Failed due to no ACL rule available(IP: < ipaddr > | < ipv6addr >, MAC: <macaddr>, Port <portNum>)	Warning	
	Port enter IMPB block state	Port <portNum> enter IMPB block state	Warning	
	Port recover from IMPB block state	Port <portNum> recover from IMPB block state	Warning	
	Dynamic IMPB entry is conflict with static NDP	Dynamic IMPB entry is conflict with static NDP(IP: <ipv6addr>, MAC: <macaddr>, Port <portNum>	Warning	
IP and Password Changed	IP Address change activity	Management IP address was changed by (Username:	Informational	

		<username>,IP:<ipaddr>,MAC:<macaddr>)		
	Password change activity	Password was changed by (Username: <username>,IP:<ipaddr>,MAC:<macaddr>)	Informational	
Dual Configuration	Excution error encountered druring system boot-up	Configuration had <int> syntax error and <int> execute error	Warning	
Safeguard Engine	Safeguard Engine is in normal mode	Safeguard Engine enters NORMAL mode	Informational	
	Safeguard Engine is in filtering packet mode	Safeguard Engine enters EXHAUSTED mode	Warning	
Packet Storm	Broadcast strom occurrence	Port <portNum> Broadcast storm is occurring	Warning	
	Broadcast storm cleared	Port <portNum> Broadcast storm has cleared	Informational	
	Multicast storm occurrence	Port <portNum> Multicast storm is occurring	Warning	
	Multicast storm cleared	Port <portNum> Multicast storm has cleared	Informational	
	Port shut down due to a packet storm	Port <portNum> is currently shut down due to a packet storm	Warning	
JWAC	When a client host authenticated successful	JWAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Informational	
	When a client host fails to authenticate	JWAC unauthenticated user (User Name: <string>, IP: <ipaddr>,	Warning	

		MAC: <macaddr>, Port: <portNum>)		
WAC	When a client host authenticated successful	WAC authenticated user (Username: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Informational	
	When a client host fails to authenticate	WAC unauthenticated user (User Name: <string>, IP: <ipaddr>, MAC: <macaddr>, Port: <portNum>)	Warning	
Loopback Detection	Port loop occurred	Port <portNum> LBD loop occurred. Port blocked.	Critical	
	Port loop detection restarted after interval time	Port <portNum> LBD port recovered. Loop detection restarted.	Informational	
	Port with VID loop occurred	Port <portNum> VID vvlanID> LBD loop occurred. Packet discard begun.	Critical	
	Port with VID Loop detection restarted after interval time	Port <portNum> VID <vlanID> LBD recovered. Loop detection restarted.	Informational	
RADIUS	VID assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This VID will be assigned to the port and this port will be the VLAN untagged port member.	RADIUS server <ipaddr> assigned VID :<vlanID> to port <portNum> (account :<username>)	Informational	Parameters description: ipaddr: The IP address of the RADIUS server. vlanID: The VID of RADIUS assigned VLAN. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.
	Ingress bandwidth	RADIUS server	Informational	Parameters description:

	assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This Ingress bandwidth will be assigned to the port.	<ipaddr> assigned ingress bandwith :<ingressBandwidth> to port <portNum> (account : <username>)		ipaddr: The IP address of the RADIUS server. ingressBandwidth: The ingress bandwidth of RADIUS assign. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.
	Egress bandwidth assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully .This egress bandwidth will be assigned to the port.	RADIUS server <ipaddr> assigned egress bandwith :<egressBandwidth> to port <portNum> (account: <username>)	Informational	ipaddr: The IP address of the RADIUS server. egressBandwidth: The egress bandwidth of RADIUS assign. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.
	802.1p default priority assigned from RADIUS server after RADIUS client is authenticated by RADIUS server successfully. This 802.1p default priority will be assigned to the port.	RADIUS server <ipaddr> assigned 802.1p default priority:<priority> to port <portNum> (account : <username>)	Informational	Parameters description: ipaddr: The IP address of the RADIUS server. priority: Priority of RADIUS assign. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated.
	Failed to assign ACL profiles/rules from RADIUS server.	RADIUS server <ipaddr> assigns <username> ACL failure at port <portNum> (<string>)	Informational	Parameters description: ipaddr: The IP address of the RADIUS server. unitID: The unit ID. portNum: The port number. Username: The user that is being authenticated. string: The failed RADIUS ACL command string.

802.1x	802.1x Authentication failure	802.1x Authentication failure [for <reason>] from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Warning	stand-alone device port <portNum> stackable device Port: <unitID:portNum>
	802.1x Authentication success	802.1x Authentication success from (Username: <username>, Port: <portNum>, MAC: <macaddr>)	Informational	stand-alone device port <portNum> stackable device Port: <unitID:portNum>
DHCP	Detect untrusted DHCP server IP address	Detected untrusted DHCP server(IP: <ipaddr>, Port: <portNum>)	Informational	
MAC-based Access Control	Login OK	MAC-AC login successful (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Informational	
	Login Fail	MAC-AC login rejected (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Warning	
	Aged out	MAC-AC host aged out (MAC: <macaddr>, port: <portNum>, VID: <vlanID>)	Informational	
Voice VLAN	When a new voice device is detected in the port	New voice device detected (Port <portNum>, MAC <macaddr>)	Informational	
	When a port which is in auto Voice VLAN mode joins the Voice VLAN	Port < portNum > add into Voice VLAN <vid >	Informational	
	When a port leaves	Port < portNum >	Informational	

	the Voice VLAN and at the same time, no voice device is detected in the aging interval for that port, the log message will be sent	remove from Voice VLAN <vid >		
DULD	The port is unidirectional	Port:<portNumver> is unidirection	Information	
Gratuitous ARP	ip conflict occure	conflict ip,mac,port,interface	information	
LLDP	LLDP-MED Topology change detected	LLDP-MED Topology change detected (on port %d. chassis id: %d, %s, port id: %d, %s, device class: %d)	notice	
	Conflict LLDP-MED device type detected	Conflict LLDP-MED device type detected (on port %d. chassis id: %d, %s, port id: %d, %s, device class: %d)	notice	
	Incompatible LLDP-MED TLV set detected	Incompatible LLDP-MED TLV set detected (on port %d. chassis id: %d, %s, port id: %d, %s, device class: %d)	notice	
PortSecurity	Address full on a port	Port security violation mac addrss %s on locking address full port %s	Warning	
BPDU-Protection	BPDU attack happened.	Port <port> enter BPDU under protection state (mode: drop / block / shutdown)	Informational	
	BPDU attack automatically recover.	Port <port> recover from BPDU under protection state	Informational	

		automatically		
	BPDU attack manually recover.	Port <port> recover from BPDU under protection state manually	Informational	
DHCPV6RELAY	Interface relay state change	DHCPv6 relay on interface %s changed state to %s	Informational	
DNSResolver	Create a host name entry which already exist in dynamic host name table	Duplicate Domain name case name: %s, static IP: %s, dynamic IP: %s	Informational	
DHCPV6Client	DHCPv6 client interface administrator state changed.	DHCPv6 client on interface <intf-name> changed state to <enabled | disabled>	Informational	
	DHCPv6 client obtains an ipv6 address from a DHCPv6 server	DHCPv6 client obtains an ipv6 address < ipv6address > on interface <intf-name>	Informational	
	The IPv6 address obtained from a DHCPv6 server starts renewing.	The IPv6 address < ipv6address > on interface <intf-name> starts renewing.	Informational	
	The IPv6 address obtained from a DHCPv6 server renews success.	The IPv6 address < ipv6address > on interface <intf-name> renews success.	Informational	
	The IPv6 address obtained from a DHCPv6 server starts rebinding.	The IPv6 address < ipv6address > on interface <intf-name> starts rebinding.	Informational	
	The IPv6 address obtained from a DHCPv6 server rebinds success.	The IPv6 address < ipv6address > on interface <intf-name> rebinds success.	Informational	
	The IPv6 address	The IPv6 address <	Informational	

	from a DHCPv6 server was deleted.	ipv6address > on interface <intf-name> was deleted.		
SD Card Managemnet	Backup failure	Backup <type>:<filename> at time <time-range> failure.	Warnning	
	Backupsuccess	Backup <type>:<filename> success at time <time-range>.	Informational	
	Execute configuration failure	Error when execute configuration <filename> line:<lineno> at time < time-range>.	Warnning	Only the first error line of configuration will be logged. If <lineno> is 0, means maybe read configuration file fail (not existed or file system error or system busy).
	Execute configuration success	Execute configuration <filename> success at time < time-range>.	Informational	

Appendix D - Trap Log Entries

This table lists the trap logs found on the DGS-3200 Series Switches.

Log Entry	Description	ID
FirmwareUpgrade	*This trap is sent when the process of upgrading the firmware via SNMP has finished.*	*1.3.6.1.4.1.171.12.1.7.2.0.7*
CfgOperCompleteTrap	*The trap is sent when the configuration is completely saved, uploaded or downloaded.*	*1.3.6.1.4.1.171.12.1.7.2.0.9*
MACNotificationTrap	*This trap indicates the MAC address variations in the address table.*	*1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.1* *1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.1* *1.3.6.1.4.1.171.11.101.3.2.100.1.2.0.1* *(DGS-3200-10/16/24)*
PortSecurityViolationTrap	*When the port security trap is enabled, new MAC addresses that violate the pre-defined port security configuration will trigger trap messages to be sent out.*	*1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.2* *1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.2* *1.3.6.1.4.1.171.11.101.3.2.100.1.2.0.2*
PortLoopOccurredTrap	*This trap is sent when a Port loop occurs.*	*1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.3* *1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.3* *1.3.6.1.4.1.171.11.101.3.2.100.1.2.0.3*
PortLoopRestart	*This trap is sent when a Port loop restarts after the interval time.*	*1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.4* *1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.4* *1.3.6.1.4.1.171.11.101.3.2.100.1.2.0.4*
VlanLoopOccurred	*This trap is sent when a Port with a VID loop occurs.*	*1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.5* *1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.5* *1.3.6.1.4.1.171.11.101.3.2.100.1.2.0.5*
VlanLoopRestart	*This trap is sent when a Port with a VID loop restarts after the interval time.*	*1.3.6.1.4.1.171.11.101.1.2.100.1.2.0.6* *1.3.6.1.4.1.171.11.101.2.2.100.1.2.0.6* *1.3.6.1.4.1.171.11.101.3.2.100.1.2.0.6*
SafeGuardChgToExhausted	*This trap indicates System change operation mode from normal to exhausted.*	*1.3.6.1.4.1.171.12.19.4.1.0.1*
SafeGuardChgToNormal	*This trap indicates System change operation mode from exhausted to normal.*	*1.3.6.1.4.1.171.12.19.4.1.0.2*

PktStormOccurred	*This trap is sent when a packet storm is detected by the packet storm mechanism and takes shutdown as an action.*	*1.3.6.1.4.1.171.12.25.5.0.1*
PktStormCleared	*This trap is sent when the packet storm is cleared by the packet storm mechanism.*	*1.3.6.1.4.1.171.12.25.5.0.2*
swPktStormDisablePort	*The trap is sent when the port is disabled by the packet storm mechanism.*	*1.3.6.1.4.1.171.12.25.5.0.3*
swIpMacBindingViolationTrap	*When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out.*	*1.3.6.1.4.1.171.12.23.5.0.1*
swIpMacBindingIPv6ViolationTrap	*When the IP-MAC Binding trap is enabled, if there's a new MAC that violates the pre-defined IPv6 IP-MAC Binding configuration, a trap will be sent out.*	*1.3.6.1.4.1.171.12.23.5.0.4*
MacBasedAuthLoggedSuccess	*This trap is sent when a MAC-based access control host is successfully logged in.*	*1.3.6.1.4.1.171.12.35.11.1.0.1*
MacBasedAuthLoggedFail	*This trap is sent when a MAC-based access control host login fails.*	*1.3.6.1.4.1.171.12.35.11.1.0.2*
MacBasedAuthAgesOut	*This trap is sent when a MAC-based access control host ages out.*	*1.3.6.1.4.1.171.12.35.11.1.0.3*
FilterDetectedTrap	*This trap is sent when an illegal DHCP server is detected. The same illegal DHCP server IP address detected is just sent once to the trap receivers within the log ceasing unauthorized duration.*	*1.3.6.1.4.1.171.12.37.100.0.1*
SingleIPMSColdStart	*The commander switch will send swSingleIPMSColdStart notification to the indicated*	*1.3.6.1.4.1.171.12.8.6.0.11*
SingleIPMSWarmStart	*The commander switch will send swSingleIPMSWarmStart*	*1.3.6.1.4.1.171.12.8.6.0.12*

	notification to the indicated host when its member generates a warm start notification.	
SingleIPMSLinkDown	*The commander switch will send swSingleIPMSLinkDown notification to the indicated host when its member generates a link down notification.*	*1.3.6.1.4.1.171.12.8.6.0.13*
SingleIPMSLinkUp	*The commander switch will send swSingleIPMSLinkUp notification to the indicated host when its member generates a link up notification.*	*1.3.6.1.4.1.171.12.8.6.0.14*
SingleIPMSAuthFail	*The commander switch will send swSingleIPMSAuthFail notification to the indicated host when its member generates an authentication failure notification*	*1.3.6.1.4.1.171.12.8.6.0.15*
SingleIPMSnewRoot	*The commander switch will send swSingleIPMSnewRoot notification to the indicated host when its member generates a new root notification.*	*1.3.6.1.4.1.171.12.8.6.0.16*
SingleIPMSTopologyChange	*The commander switch will send swSingleIPMSTopologyChange notification to the indicated host when its member generates a topology change notification.*	*1.3.6.1.4.1.171.12.8.6.0.17*
coldStart	*A coldStart trap signifies that the sending protocol entity is reinitializing itself such that the agent's configuration or the protocol entity implementation may be altered.*	*1.3.6.1.6.3.1.1.5.1*
warmStart	*A warmStart trap signifies that the sending protocol entity is reinitializing itself such that neither the agent configuration nor the protocol entity implementation is*	*1.3.6.1.6.3.1.1.5.2*

	altered.	
linkDown	*A linkDown trap signifies that the sending protocol entity recognizes a failure in one of the communication links represented in the agent's configuration.*	*1.3.6.1.6.3.1.1.5.3*
linkUp	*A linkUp trap signifies that the sending protocol entity recognizes that one of the communication links represented in the agent's configuration has come up.*	*1.3.6.1.6.3.1.1.5.4*
authenticationFailure	*An authenticationFailure trap signifies that the sending protocol entity is the address of a protocol message that is not properly authenticated.While implementations of the SNMP must be capable of generating this trap, they must also be capable of suppressing the emission of such traps via an implementation- specific mechanism.*	*1.3.6.1.6.3.1.1.5.5*
newRoot	*The newRoot trap indicates that the sending agent has become the new root of the Spanning Tree; the trap is sent by a bridge soon after its election as the new root, e.g., upon action of the Topology Change Timer immediately subsequent to its election. Implementation of this trap is optional.*	*1.3.6.1.2.1.17.0.1*
topologyChange	*A topologyChange trap is sent by a bridge when any of its configured ports transitions from the Learning state to the Forwarding state, or from the Forwarding state to the Blocking state. The trap is not sent if a newRoot trap is sent for the same*	*1.3.6.1.2.1.17.0.2*

	transition. Implementation of this trap is optional.	
PowerFailure	*The PowerFailure trap indicates that at least one power supply has failed.*	*1.3.6.1.4.1.171.12.11.2.2.2.0.2 (only DGS-3200-24)*
PowerRecover	*The PowerRecover trap indicates that the failed power is recovered.*	*1.3.6.1.4.1.171.12.11.2.2.2.0.3 (only DGS-3200-24)*
FanFailure	*The FanFailure trap indicates that any fan fails*	*1.3.6.1.4.1.171.12.11.2.2.3.0.1 (DGS-3200-16/24)*
FanRecover	*The FanRecover trap indicates that the failed fan is recovered.*	*1.3.6.1.4.1.171.12.11.2.2.3.0.2 (DGS-3200-16/24)*
agentGratuitousARPTrap	*This trap is sent when there is an IP address conflict.*	*1.3.6.1.4.1.171.12.1.7.2.0.5*
ifMauJabberTrap	*This trap is sent whenever a managed interface MAU enters the jabber state.The agent MUST throttle the generation of consecutive ifMauJabberTraps so that there is at least a five-second gap between them.*	*1.3.6.1.2.1.26.0.2*
lldpRemTablesChange	*This trap is initialed when a LLDP entry is added to or deleted from remote DB.*	*1.0.8802.1.1.2.0.0.1*
lldpXMedTopologyChangeDetected	*A notification generated by the local device sensing a change in the topology that indicates that a new remote device attached to a local port, or a remote device disconnected or moved from one port to another.*	*1.0.8802.1.1.2.1.5.4795.0.1*
swBpduProtectionUnderAttackingTrap	*The Bpdu protection under attacking trap indicates that BPDU attack happened, enter drop / block / shutdown mode.*	*1.3.6.1.4.1.171.12.76.4.0.1*
swBpduProtectionRecoveryTrap	*The Bpdu protection recovery trap indicates that BPDU attack automatically recover.*	*1.3.6.1.4.1.171.12.76.4.0.2*