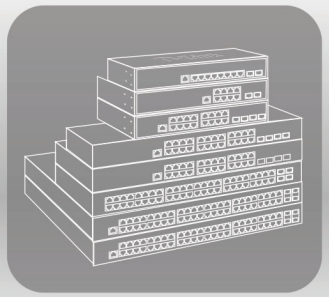
D-Link
Building Networks for People



CLI Reference Guide

Product Model : DGS-1210 v.R1 Series
Metro Ethernet Switches
Release 1.00

FCC Warning

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with this user's guide, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at hisown expense.

CE Mark Warning

This is a Class A product. In a domestic environment, this product may cause radio interference in which case the user may be required to take adequate measures.

Warnung!

Dies ist ein Produkt der Klasse A. Im Wohnbereich kann dieses Produkt Funkstoerungen verursachen. In diesem Fall kann vom Benutzer verlangt werden, angemessene Massnahmen zu ergreifen.

Precaución!

Este es un producto de Clase A. En un entorno doméstico, puede causar interferencias de radio, en cuyo case, puede requerirse al usuario para que adopte las medidas adecuadas.

Attention!

Ceci est un produit de classe A. Dans un environnement domestique, ce produit pourrait causer des interférences radio, auquel cas l`utilisateur devrait prendre les mesures adéquates.

Attenzione!

Il presente prodotto appartiene alla classe A. Se utilizzato in ambiente domestico il prodotto può causare interferenze radio, nel cui caso è possibile che l`utente debba assumere provvedimenti adeguati.

VCCI Warning

この装置は、クラス A 情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。 **VCCI-A**

December, 2019

Table of Contents

1

INTRODUCTION

DGS-1210 Rev.R1 series includes DGS-1210-10, DGS-1210-10P, DGS-1210-10MP, DGS-1210-20, DGS-1210-26, DGS-1210-28, DGS-1210-28P, DGS-1210-28MP, DGS-1210-52, DGS-1210-52MP. This series offer variable combaination of port quantity and PoE capability.

The Switch can be managed through 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. Configuration and management of the Switch via the Web-based management agent is discussed in the Web UI Refernece Guide. For detailed information on installing hardware please refer also to the Manual.

No flow controThis manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the Manual. For detailed information on installing hardware please refer also to the Manual.

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.

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

Alternatively, users 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-1210-10MP:5# config ipif System ipaddress 10.90.90.91/8
Command: config ipif System ipaddress 10.90.90.91/8


Success.
```

Figure 1–1 Assigning an IP Address

In the above example, the Switch was assigned an IP address of 10.90.90.91 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.

2

USING THE COMMAND LINE INTERFACE

The Switch allows a computer or terminal to perform some basic monitoring and configuration tasks by using the Command Line Interface (CLI) via TELNET protocol.

NOTE: Switch configuration settings are saved to non-volatile RAM using the save command. The current configuration will then be retained in the Switch's NV-RAM, and reloaded when the Switch is rebooted. If the Switch is rebooted without using the save command, the last configuration saved to NV-RAM is loaded.

The command line functions are accessed over a Telnet interface. Once an IP address for the Switch has been set, A Telnet program can be used (in VT-100 compatible terminal mode) to access and control the Switch.

The login messag contains the information of firmware verion and model name:

```
DGS-1210-28MP Gigabit Ethernet Switch
Command Line Interface

Firmware: Build 2.00.005
Copyright(C) 2019 D-Link Corporation . All rights reserved.

DGS-1210-28MP login:
```

Figure 2–1 Initial Console Screen after Logging In

Commands are entered at the command prompt, DGS-1210-28MP:5#

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

```
DGS-1210-28MP:5# ?
Command: ?


USEREXEC commands :
?
boot imageid
cable diagnostic port
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear ethernet_oam ports
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mld_snooping statistics counter
clear port_security_entry port
clear tech support
```

```
compute dlink-SHA1
config 802.1x auth_mode
config 802.1x auth_parameter ports
```

Figure 2–2 The ? Command

CLI engine offers mechanism to automatic listed the possible parameters if command does not completed entered by use:

```
DGS-1210-28MP:5# config vlan

Command: config vlan

Next possible completions :
vlanid          <vlan_name 20>

DGS-1210-28MP:5# boot

Command: boot

Next possible completions :
imageid

DGS-1210-28MP:5#
```

Figure 2–3 Example Command Parameter Help

In this case, the command config account was entered with the parameter <username>. The CLI will then prompt to enter the <username> with the message, command: config account. 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 pressing the ? key.

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

```
DGS-1210-28MP:5# config vlan

Command: config vlan

Next possible completions :
vlanid          <vlan_name 20>

DGS-1210-28MP:5#
```

Figure 2–4 Using the Up Arrow to Re-enter a Command

In the above example, the command config account was entered without the required parameter <username>, the CLI returned the command: config account 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. The < > can also indicate a word with a number for character allowed.

If a command is entered that is unrecognized by the CLI, the top-level commands are displayed under the Available commands:

```
DGS-1210-28MP:5# DLINK

Available commands :
?           boot        cable       clear
compute     config      create      delete
disable     download    enable      logout
ping        ping6       reboot      reset
save        show        traceroute  upload


DGS-1210-28MP:5#
```

Figure 2–5 Available Commands

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.

```
DGS-1210-28MP:5# show

Command: show

Next possible completions :
802.1p              802.1x              access_profile      account
acct_client         address_binding     arpentry            asymmetric_vlan
auth_client         authen              authen_enable       authen_login
authen_policy       auto_fdb            autoconfig          autoimage
bandwidth_control   command             command_history
community_encryption                    config              cos
cpu                 cpu_access_profile  ddp                 dhcp_local_relay
dhcp_relay          dhcpv6_relay        dos_prevention      dscp_mapping
duld                EEE_mode            error               ethernet_oam
fdb                 firmware            flood_fdb           greeting_message
igmp                igmp_snooping       ipif                iproute
ipv6                ipv6route           jumbo_frame         lacp
limited_multicast_addr                  link_aggregation    lldp
log                 log_save_timing     log_software_module logintimeout
loopdetect          mac_notification    management          max_mcast_group
mcast_filter_profile                    mirror              mld_snooping
multicast           multicast_fdb       packet              poe
port_priority       port_security       port_vlan           ports
power_saving        pppoe               pvid                qinq
qos                 radius              rmon                router_ports
safeguard_engine    scheduling          scheduling_mechanism
```

```
session                snmp                sntp                statistics
stp                    surveillance_vlan   switch              syslog
tech                   time                time_range          traffic
traffic_segmentation                       trusted_host        utilization
vlan                   vlan_translation    voice_vlan

DGS-1210-28MP:5#
```

Figure 2–6 Next possible completions: Show Command

In the above example, all of the possible next parameters for the show command are displayed. At the next command prompt in the example, 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.

3

COMMAND SYNTAX

The following symbols are used to describe how command entries are made and values and arguments are specified in this manual. The online help contained in the CLI and available through the Telnet uses the same syntax.

NOTE: All commands are case-sensitive. Be sure to disable Caps Lock or any other unwanted function that changes text case.

<angle brackets>	
Purpose	Encloses a variable or value that must be specified.
Syntax	**create account [admin | oper |user] <username 15>**
Description	In the above syntax example, supply a username in the <username> space. Do not type the angle brackets.
Example Command	**create account admin newadmin1**

[square brackets]	
Purpose	Encloses a required value or set of required arguments. One value or argument can be specified.
Syntax	**create account [admin | oper |user] <username 15>**
Description	In the above syntax example, specify **admin, oper** or a **user** level account to be created. Do not type the square brackets.
Example Command	**create account user newuser1**

| vertical bar	
Purpose	Separates two or more mutually exclusive items in a list, one of which must be entered.
Syntax	**create account [admin | oper | user] <username 15>**
Description	In the above syntax example, specify **admin, oper,** or **user**. Do not type the vertical bar.
Example Command	**create account user newuser1**

All commands are case-sensitive. Be sure to disable Caps Lock or any other unwanted function that changes text case.

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	reset
Description	execute “reset” will return the switch to its factory default setting.
Example command	reset Please be aware that all configuration will be reset to default value. Are you sure you want to proceed with system reset now? (Y/N)[N] N

Line Editing Key Usage	
Delete	Deletes the character under the cursor and then shifts the remaining characters in the line to the left.
Backspace	Deletes the character to the left of the cursor and then shifts the remaining characters in the line to the left.
Insert or Ctrl+R	Toggle on and off. When toggled on, inserts text and shifts previous text to the right.
Left Arrow	Moves the cursor to the left.
Right Arrow	Moves the cursor to the right.
Up Arrow	Repeats the previously entered command. Each time the up arrow is pressed, the command previous to that displayed appears. This way it is possible to review the command history for the current session. Use the down arrow to progress sequentially forward through the command history list.
Down Arrow	The down arrow displays the next command in the command history entered in the current session. This displays each command sequentially as it was entered. Use the up arrow to review previous commands.
Tab	Shifts the cursor to the next field to the left.

Multiple Page Display Control Keys	
Space	Displays the next page.
CTRL+c	Stops the display of remaining pages when multiple pages are to be displayed.
ESC	Stops the display of remaining pages when multiple pages are to be displayed.
n	Displays the next page.
p	Displays the previous page.
q	Stops the display of remaining pages when multiple pages are to be displayed.
r	Refreshes the pages currently displayed.
a	Displays the remaining pages without pausing between pages.
Enter	Displays the next line or table entry.

4

BASIC SWITCH COMMANDS

The Basic Switch commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable password encryption	
disable password encryption	
create account	[admin | operator | user] <username 15>
config account	<username 15> {encrypt {plain_text <password 15> | sha_1 <password 35>}}
show account	
reset account	
reset password	{<username 15>}
delete account	<username 15>
show session	
show switch	
enable web	{<tcp_port_number 1-65535>}
disable web	
enable autoconfig	
disable autoconfig	
show autoconfig	
show config	[[config_in_nvram config_id <value 1-2>] | current_config] [begin | exclude] <string 80>
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	
save	[config | log]
reboot	
reset system	{[include | force_agree]}
logout	
ping	{times <value 0-255> | timeout <sec 1-99> | size <value 1-60000>}
ping6	<ipv6_addr> {size <value 1-6000> | timeout <sec 1-99> | times <value 1-255>}
enable telnet	{<tcp_port_number 1-65535>}
disable telnet	

Command	Parameter
config time_range	<range_name 20> [hours start_time <start_time 32> end_time <end_time 32> weekdays <daylist 32> date from_day year <start_year 2011-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2011-2029> month <end_mth 1-12> date <end_date 1-31> | delete]
show time_range	

Each command is listed in detail, as follows:

enable password encryption

Purpose	Used to enable password encryption on a user account.
Syntax	**enable password encryption**
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To enable password encryption on the Switch:

```
DGS-1210-28MP:5# enable password encryption
Command: enable password encryption


Success.

DGS-1210-28MP:5#
```

disable password encryption

Purpose	Used to disable password encryption on a user account.
Syntax	**disable password encryption**
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system at a time in the future. If the password encryption is enabled, the password will be in encrypted form. If password encryption is disabled and the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enabled password encryption command, the password will still be in encrypted form. It can not revert back to plain text.
Parameters	None.

Restrictions	Only Administrat level users can issue this command.

Example usage:

To disable password encryption on the Switch:

```
DGS-1210-28MP:5#  disable password encryption
Command: disable password encryption

Success !
DGS-1210-28MP:5#
```

create account

Purpose	To create user accounts.
Syntax	**create account [admin | operator | user] <username 15>**
Description	The **create account** command creates an administrator, operator, or user account that consists of a username and an optional password. Up to 31 accounts can be created. You can enter username and Enter. In this case, the system prompts for the account's password, which may be between 0 and 15 characters. Alternatively, you can enter the username and password on the same line.
Parameters	*admin* − Name of the administrator account. *oper* − Specify an operator level account. *user* − Specify a user account with read-only permissions. <*username 1-15*> − The account username may be between 1 and 15 characters. *password* <password_string> {encrypted} - the account password can be included, and (optionally) can be encrypted.
Restrictions	Only Administrator level users can issue this command. Usernames can be between 1 and 15 characters. Passwords can be between 0 and 15 characters.

NOTE: You are not required to enter a User Name. However, if you do not enter a User Name, you cannot perform the following actions:

Create a monitor or operator (level 1 or level 14) users until an administrator user (level 15) is defined.

Delete the last administrator user if there are monitor and/or operator users defined.

Example usage:

To create an administrator-level user account with the username 'dlink':

```
DGS-1210-28MP:5# create account admin dlink
Command: create account admin dlink

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

Success.
```

DGS-1210-28MP:5#

config account

Purpose	To change the password for an existing user account.
Syntax	**config account <username 15> {encrypt {plain_text <password 15> | sha_1 <password 35>}}**
Description	The **config account** command changes the password for a user account that has been created using the **create account** command. The system prompts for the account's new password, which may be between 0 and 15 characters.
Parameters	*<username 15>* − the account username. *encrypt* – Capbility for option <plain text> or <sha 1> encryption *sha_1* – Encryption method (password string can be hashed via command "compute dlink-sSHA1 <string15>)
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of 'dlink' account:

```
DGS-1210-28MP:5# compute dlink-SHA1 test
Command: compute dlink-SHA1 test

Result = *@&qUqP5cyxm6YcTAhz05Hph5gvu9P+CdlY

DGS-1210-28MP:5# config account dlink encrypt sha_1 *@&qUqP5cyxm6Y
cTAhz05Hph5gvu9P+CdlY
Command: config account dlink encrypt sha_1 ******

DGS-1210-28MP:5# show config current_config include "account"
Command: show config current_config include account

#------------------------------------------------------------------------
#            DGS-1210-28MP Gigabit Ethernet Switch Configuration
#
#                        Firmware: Build 2.00.005
#       Copyright(C) 2019 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
create account admin "dlink"
*@&qUqP5cyxm6YcTAhz05Hph5gvu9P+CdlY
*@&qUqP5cyxm6YcTAhz05Hph5gvu9P+CdlY
```

show account

Purpose	To display information about all user accounts on the Switch.
Syntax	**show account**
Description	The **show account** command displays all account usernames and their access levels created on the Switch. Up to 31 user accounts can exist on the Switch at one time.

Parameters	None.
Restrictions	None.

Example usage:

To display the created account information

```
DGS-1210-28MP:5# show account
Command: show account

Username         Access Level
---------------- ------------
dlink            Admin

Total Entries    : 1

DGS-1210-28MP:5#
```

reset account

Purpose	To erase entire account information
Syntax	**reset account**
Description	The **reset account** command is used to erase ALL accounts information.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To reset all accounts created:

```
DGS-1210-28MP:5# reset account
Command: reset account

Are you sure to proceed with clean account?(y/n)y

Success.

DGS-1210-28MP:5#
```

reset password

Purpose	To erase the password configured in user accounts
Syntax	**reset password {<username 15>}**
Description	The **reset passowrd** command is used to erase ALL or particular password information configured in user accounts.
Parameters	*<username 15>* - Specify the user account the password would be reset. Without this parameter, ALL account password would be reset.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To reset password in ALL accounts :

```
DGS-1210-28MP:5# reset password
Command: reset password


Success.

DGS-1210-28MP:5#
```

delete account

Purpose	To delete an existing user account.
Syntax	**delete account <username 15>**
Description	The **delete account** command deletes a user account that has been created using the **create account** command.
Parameters	*<username 15>* − the account username.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account 'System':

```
DGS-1210-28MP:5# delete account dlink
Command: delete account dlink


Success.

DGS-1210-28MP:
```

show session

Purpose	To display information about currently logged-in users.
Syntax	**show session**
Description	The **show session** command displays a list of all the users that are logged-in at the time the command is issued. The information includes the session ID (0 for the first logged-in user, 1 for the next logged-in user, etc.), the Protocol used to connect to the Switch, the user's IP address, the user's access Level (1=user, 15=admin), and the account name on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display logged in user information:

```
DGS-1210-28MP:5# show session
Command: show session

ID   Login Time          Live Time     From            Level   Name
```

```
--   -------------------     ------------    ---------------   -----   ---------------
2    1/1/2019 05:53:24    00:00:07    10.90.90.123    5     dlink


Total Entries      : 1

DGS-1210-28MP:5#
```

show switch

Purpose	To display information about the Switch.
Syntax	**show switch**
Description	The **show switch** command displays information about the Switch settings, including Device Type, MAC Address, IP configuration, Hardware/Software version, System information, and Switch Network configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch information:

```
DGS-1210-28MP:5# show switch
Command: show switch

Device Type                    : DGS-1210-28MP
MAC Address                    : EC-AD-E0-62-AF-A0
IP Address                     : 10.90.90.90
VLAN Name                      : default
Subnet Mask                    : 255.0.0.0
Default Gateway                : 0.0.0.0
System Boot Version            : 2.00.004
System Firmware Version        : 2.00.005
System Hardware Version        : R1
System Serial Number           : QBDES12105200
System Name                    :
System Location                :
System Up Time                 : 0 days, 5 hrs, 55 min, 17 secs
System Contact                 :
System Time                    : 05:55:40 01 01 2019
IGMP Snooping                  : Disabled
802.1X Status                  : Disabled
Telnet                         : Enabled  <TCP  23>
SSH                            : Enabled  <TCP  22>
Web                            : Enabled  <TCP  80>
RMON                           : Disabled
Syslog Global State            : Disabled
CLI Paging                     : Enabled
```

```
DGS-1210-28MP:5#
```

enable web

Purpose	To enable the HTTP-based management software on the Switch.
Syntax	**enable web {<tcp_port_number 1-65535>}**
Description	The **enable web** command enables the Web-based management software on the Switch. The user can specify the TCP port number the Switch uses to listen for Telnet requests.
Parameters	*<tcp_port_number 1-65535>* − The TCP port number. TCP ports are numbered between 1 and 65535. The 'well-known' port for the Web-based management software is 80.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable HTTP or configure the TCP port number:

```
DGS-1210-28MP:5# enable web
Command: enable web


Success.

DGS-1210-28MP:5# enable web 9527
Command: enable web 9527


Success.

DGS-1210-28MP:5#
```

disable web

Purpose	To disable the HTTP-based management software on the Switch.
Syntax	**disable web**
Description	The **disable web** command disables the Web-based management software on the Switch. Please be noted disabling HTTP access method may cause lost management if this is the LAST management method available.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable HTTP-capbility of switch:

```
DGS-1210-28MP:5# disable web
Command: disable web
```

```
Success.

DGS-1210-28MP:5#
```

enable autoconfig

Purpose	Used to activate the auto configuration function for the Switch. This will load a previously saved configuration file for current use.
Syntax	**enable autoconfig**
Description	When autoconfig is enabled on the Switch, the DHCP reply will contain a configuration file and path name. It will then request the file from the TFTP server specified in the reply. When autoconfig is enabled, the ipif settings will automatically become DHCP client.
Parameters	None.
Restrictions	When autoconfig is enabled, switch turned into DHCP client mode AUTOMATICALLY after device reboot. Please be aware the DHCP server MUST capable to transmit the following options: DHCP option6 (Domain Name Server.), option 66 (TFTP server name), option 67 (Bootfile name), and option 150 (TFTP Server Address) with the correct contents which guide the swtich to contact the TFTP server and obtain the config file. If the switch failed to complete the autoconfig process, the origin config will be used after process timed out.

Example usage:

To enable auto configuration on the Switch:

```
DGS-1210-28MP:5# enable autoconfig
Command: enable autoconfig

Success.
DGS-1210-28MP:5#
```

disable autoconfig

Purpose	Use this to deactivate auto configuration from DHCP.
Syntax	**disable autoconfig**
Description	The **disable autoconfig** command is used to instruct the Switch not to accept auto configuration instruction from the DHCP server. This does not change the IP settings of the Switch. The ipif settings will continue as DHCP client until changed with the config ipif command.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command. .

Example usage:

To stop the auto configuration function:

```
DGS-1210-28MP:5# disable autoconfig
Command: disable autoconfig
```

```
Success.

DGS-1210-28MP:5#
```

config autoconfig timeout

Purpose	Used to configure the timeout period.
Syntax	**config autoconfig timeout <integer 1-65535>**
Description	The **config autoconfig** command is used to configure the time out range from 1~65535 seconds.
Parameters	*<1-65535>* - Specify the timeout range from 1~65535 seconds
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DGS-1210-28MP:5# config autoconfig timeout 300
Command: config autoconfig timeout 300


Success.

DGS-1210-28MP:5#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	**show autoconfig**
Description	The **show autoconfig** command is used to list the current status of the auto configuration function.
Parameters	None.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
DGS-1210-28MP:5# show autoconfig
Command: show autoconfig

Autoconfig State: Disabled
Timeout        : 300 sec


Success.
DGS-1210-28MP:5#
```

show config

Purpose	To display the current or saved version of the configuration settings of the Switch.
Syntax	**show config [[config_in_nvram config_id <value 1-2>] | current_config] [begin | exclude | include] <string 80>**
Description	The **show config** command is used to list the current status of the configuration settings of the Switch.
Parameters	config_in_nvram config_id <value 1-2> − Display the system configuration from NV-RAM. current_config − Display system configuration from the DRAM database, i.e. the current system setting. [begin | exclude | include] − Display the configuration which is begined, excluded or included. <string 80> − Display the configuration which begin or exclude the specified string. The maximum string is 80.
Restrictions	None.

Example usage:

To display current config in switch:

```
DGS-1210-28MP:5# show config current_config
Command: show config current_config

#------------------------------------------------------------------------
#            DGS-1210-28MP Gigabit Ethernet Switch Configuration
#
#                        Firmware: Build 2.00.005
#        Copyright(C) 2019 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------
command-start

# Port
config ports 1-28 speed auto
config ports 25-28 medium_type fiber speed auto
config ports 1-28 state enable
config ports 25-28 medium_type fiber state enable
config ports 1-28 flow_control disable
config ports 25-28 medium_type fiber flow_control disable
config ports 1-28 learning enable
config ports 25-28 medium_type fiber learning enable
config ports 1-28 mdix auto
config ports 1 capability_advertised 10_half 10_full 100_half 100_full 1000_full
config ports 2 capability_advertised 10_half 10_full 100_half 100_full 1000_full
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

enable jumbo_frame

Purpose	To enable jumbo frames on the device.

Syntax	**enable jumbo_frame**
Description	The **enable jumbo_frame** command enables jumbo frames on the device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To enable jumbo frames:

```
DGS-1210-28MP:5# enable jumbo_frame
Command: enable jumbo_frame

Success.

DGS-1210-28MP:5#
```

disable jumbo_frame

Purpose	To disable jumbo frames on the device.
Syntax	**disable jumbo_frame**
Description	The **disable jumbo_frame** command disables jumbo frames on the device.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable jumbo_frames:

```
DGS-1210-28MP:5# disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-1210-28MP:5#
```

show jumbo_frame

Purpose	To display the jumbo frame configuration.
Syntax	**show jumbo_frame**
Description	The **show jumbo_frame** command displays the jumbo frame configuration.
Parameters	None.
Restrictions	None.

Example usage:

To show the jumbo_frames capability:

```
DGS-1210-28MP:5# show jumbo_frame
```

```
Command: show jumbo_frame

Jumbo Frame is  Enabled
DGS-1210-28MP:5#
```

save

Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	**save [config> | log]**
Description	The **save** command used to enter the current switch configuration into non-volatile RAM. The saved switch configuration will be loaded into the Switch's memory each time the Switch is restarted.
Parameters	*config* – Used to save the current configuration to a file. *log* – Used to save the current log to a file. The log file cannot be deleted.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To save current configurations into non-volatile RAM:

```
DGS-1210-28MP:5# save config
Command: save config



Success.

DGS-1210-28MP:5#
```

reboot

Purpose	To reboot the Switch.
Syntax	**reboot**
Description	The **reboot** command restarts the Switch.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To restart the Switch:

```
DGS-1210-28MP:5# reboot
Command: reboot

Are you sure you want to proceed with the system reboot?(y/n)y
```

reset

Purpose	To reset the Switch to the factory default settings.
Syntax	**reset {system} {force_agree}**

Description	The **reset** command restores the Switch's configuration to the default settings in veriable ways: 1. IP address, log and user account remains 2. Entire configuration restored to factory default
Parameters	*system* − If the keyword 'system' is specified all of the factory default settings are restored on the Switch. The Switch will save and reboot after the settings are changed to default. *{force_agree}* - When force_agree is specified, the reset command will be executed immediately without further confirmation. If no parameter is specified, the Switch's current IP address, user accounts, and the switch history log are not changed. All other parameters are restored to the factory default settings. The Switch will not save or reboot.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To restore all of the Switch's parameters to their default values:

```
DGS-1210-28MP:5# reset system
Command: reset system

Are you sure you want to proceed with the system reset, save and reboot?(y/n)
```

logout

Purpose	To log out a user from the Switch.
Syntax	**Logout**
Description	The **logout** command terminates the current user's session on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current CLI session:

```
DGS-1210-28MP:5# logout
Command: logout
```

ping

Purpose	To test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 0-255> | timeout <sec 1-99> | size <value 1-60000>}**
Description	The **ping** command sends Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address then 'echos' or returns the message. This is used to confirm connectivity between the Switch and the remote device.

Parameters	*<ipaddr>* - The IP address of the host. *times <value 0-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4. *timeout <sec 1-99>* - 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. *size <value 1-60000>* - Specify the size of the test packet. A value of 0 to 2080 can be specified.
Restrictions	None.

Example usage:

To ping the IP address 10.90.90.97 three times:

```
DGS-1210-28MP:5# ping 10.90.90.123 times 3 size 100 timeout 3
Command: ping 10.90.90.123 times 3 size 100 timeout 3

Reply Received From :10.90.90.123, TimeTaken : 40 ms
Reply Received From :10.90.90.123, TimeTaken : 20 ms
Reply Received From :10.90.90.123, TimeTaken : 40 ms

--- 10.90.90.123 Ping Statistics ---
3 Packets Transmitted, 3 Packets Received, 0% Packets Loss
DGS-1210-28MP:5#
```

ping6

Purpose	To test the IPv6 connectivity between network devices.
Syntax	**ping6 <ipv6addr> {size <value 1-6000> | timeout <sec 1-99> | times <value 1-255>}**
Description	The **ping6** command sends IPv6 Internet Control Message Protocol (ICMP) echo messages to a remote IPv6 address. The remote IPv6 address will then “echo” or return the message. This is used to confirm the IPv6 connectivity between the switch and the remote device.
Parameters	*<ipv6addr>* - The IPv6 address of the host. *size <value 1-6000>* - Specify the size of the test packet. A value of 1 to 6000 can be specified. *timeout <sec 1-99>* - 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. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. The maximum value is 255. The default is 4.
Restrictions	None.

Example usage:

To ping the IPv6 address to “3000::1” four times:

```
DGS-1210-28MP:5#ping6 3000::1 times 4
Command: ping6 3000::1 times 4

Reply From : 3000::1, bytes=200, time<10ms
Reply From : 3000::1, bytes=200, time<10ms
```

```
Reply From : 3000::1, bytes=200, time<10ms
Reply From : 3000::1, bytes=200, time<10ms


--- 3000::1 Ping Statistics ---
4 Packets Transmitted, 4 Packets Received, 0% Packets Loss
DGS-1210-28MP:5#
```

enable telnet

Purpose	To enable the telnet.
Syntax	**enable telnet {<tcp_port_number 1-65535>}**
Description	The **enable telnet** command enables telnet.
Parameters	*<tcp_port_number 1-65535>* - Specify the TCP port number for the telnet setting.
Restrictions	Only Administrator or operate-level users can issue this command

Example usage:

To enable telnet:

```
DGS-1210-28MP:5# enable telnet
Command: enable telnet


Success.

DGS-1210-28MP:5#
```

disable telnet

Purpose	To disable telnet.
Syntax	**disable telnet**
Description	The **disable telnet** command disables telnet. Please be noted disabling TELNET access method may cause lost management if this is the LAST management method available.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command

Example usage:

To disable telnet:

```
DGS-1210-28MP:5# disable telnet
Command: enable telnet

```

config time_range

Purpose	To configure the time range on the Switch.
Syntax	**config time_range <range_name 20> [[hours start_time**

	<start_time 32> end_time <end_time 32> weekdays <daylist 32> date from_day year <start_year 2014-2029> month <start_mth 1-12> date <start_date 1-31> to_day year <end_year 2014-2029> month <end_mth 1-12> date <end_date 1-31>] | delete]
Description	The **config time_range** command defines time ranges for access lists. If the end time is earlier than the start time, the end time will move to the following day
Parameters	*<range_name 20>* – Specifies the time range name. The range of characters is 1 - 20. *start_time <start_time 32>* – defines the time on which the time range will start to be active. *end_time <end_time 32 >*– defines the time on which the time range will stop to be active. *weekdays <daylist 32>* – defines the days of the week on which the time range will be active. *<start_year 2014-2029 >* – Specifies the time range start year. *<start_mth 1-12>* – Specifies the time range start month. *<start_date 1-31>* – Specifies the time range start date. *<end_year 2014-2029 >* – Specifies the time range end year. *<end _mth 1-12>* – Specifies the time range end month. *<end _date 1-31>* – Specifies the time range end date. *delete* – Delete the time range settings.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the time range on the Switch:

DGS-1210-28MP:5# config time_range test hours start_time 00:33 end_time 15:30 weekdays mon,tue,wed,thu,fri,sat,sun

Command: config time_range test hours start_time 00:33 end_time 15:30 weekdays mon,tue,wed,thu,fri,sat,sun

Success.

show time_range

Purpose	To display the currently configured access profiles on the Switch.
Syntax	**show time_range**
Description	The **show time_range** command displays the time range configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display time range settings on the Switch:

```
DGS-1210-28MP:5# show time_range
Command: show time_range


Time Range Information
---------------------------------------------
Range Name                : test
Weekdays                  : mon,tue,wed,thu,fri,sat,sun
Start Time                : 00:33
End Time                  : 15:30
From Day                  :
To Day                    :
```

5

MODIFY BANNER AND PROMPT COMMANDS

The Modify Banner and Prompt commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config command_prompt	[<string 32> | default | username]
config greeting_message	{default}
show greeting_message	

Each command is listed in detail, as follows:

config command_prompt	
Purpose	To configure the command prompt.
Syntax	**config command_prompt [<string 32> | default | username]**
Description	The **config command_prompt** command configures the command prompt.
Parameters	*<string 32>* – The command prompt can be changed by entering a new name of no more that 32 characters. *default* – The command prompt will reset to factory default command prompt. Default = the name of the Switch model, for example "DGS-1210-28MP". *username* – The command prompt will be changed to the login username.
Restrictions	Only Administrator-level users can issue this command. Other restrictions include: If the "reset" command is executed, the modified command prompt will remain modified. However, the "reset config/reset system" command will reset the command prompt to the original factory banner.

Example usage:

Change the command prompt to username:

```
DGS-1210-28MP:5# config command_prompt username
Command: config command_prompt username


Success.

dlink:5#
```

config greeting_message	
Purpose	Used to configure the login banner (greeting message).
Syntax	**config greeting_message {default}**
Description	The **config greeting_message** command to modify the login banner (greeting message).
Parameters	*default* – If the user enters default to the modify banner command, then the banner will be reset to the original factory banner. To open the Banner Editor, click Enter after typing the config greeting_message command. Type the information to be displayed on the banner by using the commands described on the Banner Editor: Quit without save: Ctrl+C Save and quit: Ctrl+W Move cursor: Left/Right/Up/Down Delete line: Ctrl+D Erase all setting: Ctrl+X Reload original setting: Ctrl+L
Restrictions	Only Administrator-level users can issue this command. Other restrictions include: If the “reset” command is executed, the modified banner will remain modified. However, the “reset config/reset system” command will reset the modified banner to the original factory banner. The capacity of the banner is 6*80. 6 Lines and 80 characters per line. Ctrl+W will only save the modified banner in the DRAM. Users need to type the “save config/save all” command to save it into Flash.

Example usage:

```
DGS-1210-28MP:5# config greeting_message
Command: config greeting_message

Greeting Messages Editor
============================================================
DGS-1210-28MP
DGS-1210-28MP
DGS-1210-28MP
DGS-1210-28MP
============================================================


Array Up    : Cursor up          Ctrl+X    : Erase all
Array Down  : Cursor down        Ctrl+L    : Relaod original data
Array Left  : Cursor left        Ctrl+C    : Quit without save
Array Right : Cursor right       Ctrl+W    : Save and quit
Ctrl+D      : Erase current line
```

show greeting_message	
Purpose	Used to view the currently configured greeting message configured on the Switch.
Syntax	**show greeting_message**
Description	The **show greeting_message** command is used to view the currently configured greeting message on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the currently configured greeting message:

```
DGS-1210-28MP:5# show greeting_message
Command: show greeting_message


DGS-1210-28MP
DGS-1210-28MP
DGS-1210-28MP
DGS-1210-28MP


DGS-1210-28MP:5#
```

6

SWITCH PORT COMMANDS

The Switch Port commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config ports	[all | <portlist>] medium_type [copper | fiber] MDI/MDIX [MDI | MDIX | auto] {description <desc 32> | clear_description| flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 100_full | 100_half | 10_full | 10_half]}
show ports	{[<portlist> | all] | media type | description | err_disabled | auto_negotiation | linkup_time}
config duld ports	[all | <portlist>] {state [enable | disable] | mode [shutdown | normal | discovery_time <sec 5-65535)>}
show duld ports	{all | <portlist>}

Each command is listed in detail, as follows:

config ports	
Purpose	To configure the Switch's Ethernet port settings.
Syntax	**config ports [all | <portlist>] medium_type [copper | fiber] MDI/MDIX [MDI | MDIX | auto] {description <desc 32> | clear_description| flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 100_full | 100_half | 10_full | 10_half]}**
Description	The **config ports** command configures the Switch's Ethernet port settings. Only the ports listed in the <portlist> are affected.
Parameters	*<portlist>* − A port or range of ports to be configured. *all* − Configures all ports on the Switch. *medium_type [copper | fiber]* − If configuring the Combo ports, this defines the type of medium being configured. *MDI/MDIX [MDI | MDIX | j auto]* − Specifies the MDI or MDIX setting of the port. The MDIX setting can be auto, normal or cross. If set to normal state, the port in MDIX mode, can be connected to PC NIC using a straight cable. If set to cross state, the port in mdi mode, can be connected to a port (in mdix mode) on another switch through a straight cable. *description <desc 32>* − Enter and alphanumeric string of no more that 32 characters to describe a selected port interface. *clear_description* – Clear the description for the specified ports. *flow_control [enable]* – Enables flow control for the specified ports. *flow_control [disable]* – Disables flow control for the specified ports. *learning [enable | disable]* c Enables or disables the MAC address learning on the specified range of ports. *state [enable | disable]* − Enables or disables the specified range of

	ports. *speed* – Sets the speed of a port or range of ports, with the addition of one of the following: • *auto* − Enables auto-negotiation for the specified range of ports. • *[10 | 100 | 1000]* − Configures the speed in Mbps for the specified range of ports. • *[half | full]* − Configures the specified range of ports as either full or half-duplex.
Restrictions	Only Administrator or Operator level users can issue this command.

Example usage:

To configure the speed of ports 1-3 to be 100 Mbps, full duplex, learning and state enabled:

```
DGS-1210-28MP:5# config ports 1-3 medium_type copper speed 100_full
learning enable state enable
Command: config ports 1-3 medium_type copper speed 100_full learning enable
state enable

Success.

DGS-1210-28MP:5#
```

show ports

Purpose	To display the current configuration of a range of ports.
Syntax	**show ports {[<portlist> | all] | media type | description | err_disabled | auto_negotiation | linkup_time}**
Description	The **show ports** command displays the current configuration of a port or range of ports.
Parameters	<*portlist*> − A port or range of ports whose settings are to be displayed. *all* – Specifies all ports to be displayed. *media type* – Display the media type used to estibalished connection *description* – Display the port description *error_disable* – Display the port error disable information *auto_negotiation* – Display the auto negotiation result of the port specified *linkup_time* – Display the time linked up of the port specified.
Restrictions	None.

Example usage:

To display the configuration of port 1-3 on the Switch:

```
DGS-1210-28MP:5# show ports 1-3
Command: show ports 1-3
```

Port	State/ MDI	Settings Speed/Duplex/FlowCtrl	Connection Speed/Duplex/FlowCtrl	Address Learning
1	Enabled Auto	100M/Full/Disabled	Link Down	Enabled
2	Enabled Auto	100M/Full/Disabled	Link Down	Enabled
3	Enabled Auto	100M/Full/Disabled	Link Down	Enabled

config duld ports

Purpose	To configure DULD (D-Link Unidirectional Link Detection) feature.
Syntax	**config duld ports {state [enable | disable] | mode [shutdown | normal | discovery_time <sec 5-65535)>}**
Description	D-Link Unidirectional Link Detection provides discovery mechanism based on IEEE 802.3ah to discovery its neighbor. If the discovery can complete in configured discovery time, it concludes the link is bidirectional. Otherwise, it starts detecting task to detect the unidirectional link status.
Parameters	*{all | <portlist>}* − Specifies all ports or range of ports to be configured. *state [enable | disable]* – To configure the state of DULD feature of specified port. *mode* – Specify the action when unidirectional link detected *shutdown* – shutdown the port when unidirection link detected *normal* – Only log an event when a unidirectional link is detected *discovery_time* – Specify the time for neighbor discovery. If the discovery is timeout, the unidirectional link detection will start.
Restrictions	Only Administrator level users can issue this command

Example usage:

To configure DULD feature in ports 1-5.

```
DGS-1210-28MP:5# config duld ports 1-5 state enable mode shutdown
Command: config duld ports 1-5 state enable mode shutdown


Success.
```

show duld ports

Purpose	To display the Switch's Ethernet duld port settings.
Syntax	**show duld ports {all | <portlist>}**
Description	The **show duld ports** command displays the Switch's Ethernet duld port settings.
Parameters	*{all | <portlist>}* − Specifies all ports or range of ports to be

	displayed.
Restrictions	None.

Example usage:

To display the Switch's Ethernet duld ports 1-5 settings.

```
DGS-1210-28MP:5# show duld ports 1-5
Command: show duld ports 1-5

Port  Admin State  Oper Status  Mode      Link Status    Discovery Time
----  -----------  -----------  --------- -------------  --------------
1     Enabled      Disabled     ShutDown  Unknown        5
2     Enabled      Disabled     ShutDown  Unknown        5
3     Enabled      Disabled     ShutDown  Unknown        5
4     Enabled      Disabled     ShutDown  Unknown        5
5     Enabled      Disabled     ShutDown  Unknown        5
DGS-1210-28MP:5#
```

7

LOOPBACK DETECTION COMMANDS

The Loopback Detection commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable loopdetect	
disable loopdetect	
config loopdetect mode	[portbase | vlanbase]
config loopdetect ports	[<portlist > | all] state [enable | disable]
config loopdetect	interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]
config loopdetect vlan	{all | <vidlist 1-4094>} state {disable | enable}
show loopdetect	{ports [<portlist > | all]}

Each command is listed in detail, as follows:

enable loopdetect	
Purpose	To enable the loop back detection on the Switch.
Syntax	**enable loopdetect**
Description	The **enable loopdetect** command enables the loop back detection on the Switch.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the loopback detection feature on the Switch:

```
DGS-1210-28MP:5# enable loopdetect
Command: enable loopdetect


Success.
```

disable loopdetect	
Purpose	To disable the loop back detection on the Switch.
Syntax	**disable loopdetect**
Description	The **disable loopdetect** command disables the loop back detection on the Switch.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the loopback detection feature on the Switch:

```
DGS-1210-28MP:5# disable loopdetect
Command: disable loopdetect


Success.
```

config loopdetect mode

Purpose	To configure the loop back detection mode to be portbase or vlanbase on the Switch.
Syntax	**config loopdetect mode [portbase | vlanbase]**
Description	The **config loopdetect mode** command configures loop back detection mode to be portbase or vlanbase on the Switch.
Parameters	*portbase* – The port would be physical shutdown if loop detected by LBD *vlanbase* – The port would stay on physical LINKED but the particular VLAN traffic would be dropped (The VLAN that loop detected)
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the loopback detection mode to be portabse on the Switch:

```
DGS-1210-28MP:5# config loopdetect mode vlanbase
Command: config loopdetect mode vlanbase


Success.
```

config loopdetect ports

Purpose	To configures the loop back detection to be enabled or disabled for the specific ports on the Switch.
Syntax	**config loopdetect ports [<portlist > | all] state [enable | disable]**
Description	The **config loopdetect ports** command configures the loop back detection to be enabled or disabled for the specific ports on the Switch.
Parameters	*<portlist >* − A port or range of ports to be configured. *all* − All ports settings are to be configured. *[enabled | disabled]* − Specifies the loop back detection is enabled or disabled for the specified ports on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the loop back detection on all ports

```
DGS-1210-28MP:5# config loopdetect ports all state disable
Command: config loopdetect ports all state disable
```

```
Success.
```

config loopdetect

Purpose	To configure the loop back detection interval time and recover time on the Switch.
Syntax	**config loopdetect ports interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]**
Description	The **config loopdetect** command is used to configure detection interval and recovery time.
Parameters	*interval_time <value 1-32767>* − Specifies the interval time of loop back detection. The range is between 1 and 32767 seconds. *lbd_recover_time [0 | <value 60-10000>]* − Specifies the recover time of loop back detection on the switch. "Value 0" represents recovery mechanism turned off. The range is between 60 and 10000 seconds.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the loop back detection with interval time 500 on the Switch:

```
DGS-1210-28MP:5# config loopdetect lbd_recover_time 0
Command: config loopdetect lbd_recover_time 0

Success.
```

config loopdetect vlan

Purpose	To configure the specific VLAN group for loopdetect VLAN mode.
Syntax	**config loopdetect vlan {all | <vidlist 1-4094>} state {disable | enable}**
Description	The **config loopdetect vlan** command is used to control the state of particular VLAN group.
Parameters	*vlan {all | <vidlist 1-4094>}* − Specifies the VLAN group for all or particular VID. *state {disable | enable}* – Used to control the state for specified VLAN.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

Turn on loopdect on VID 33:

```
DGS-1210-28MP:5# config loopdetect vlan 33 state enable
Command: config loopdetect vlan 33 state enable

Success.
```

show loopdetect	
Purpose	To display the loop back detection information on the Switch.
Syntax	**show loopdetect {ports [<portlist > | all]}**
Description	The **show loopdetect** command displays the loop back detection information on the Switch.
Parameters	*<portlist* > − A port or range of ports to be displayed. *all* − All ports settings are to be displayed.
Restrictions	None.

Example usage:

To display the loop back detection information on the Switch:

```
DGS-1210-28MP:5# show loopdetect
Command: show loopdetect

    Loopdetect Global Settings
    --------------------------
Loopdetect Status       : Enabled
Loopdetect Mode         : Vlan-Base
VLAN List               : 33
Loopdetect Interval     : 2
Recover Time            : 0
DGS-1210-28MP:5#
```

8

PPPOE CIRCUIT ID INSERTION COMMANDS

PPPoE Circuit ID Insertion is used to produce the unique subscriber mapping capability that is possible on ATM networks between ATM-DSL local loop and the PPPoE server. The PPPoE server will use the inserted Circuit Identifier sub-tag of the received packet to provide AAA services (Authentication, Authorization and Accounting). Through this method, Ethernet networks can be as the alternative of the ATM networks.

The PPPoE Circuit ID Insertion commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config pppoe circuit_id _insertion state	[enable | disable]
config pppoe circuit_id_insertion ports	[all | <portlist >] [circuit_id [mac | ip | udf <string 32>] | state [enable | disable]]
show pppoe circuit_id_insertion	
show pppoe circuit_id_insertion ports	{<portlist>}

Each command is listed in detail, as follows:

config pppoe circuit_id_insertion state	
Purpose	Used to enable or disable the PPPoE circuit identifier insertion.
Syntax	**config pppoe circuit_id_insertion state [enable | disable]**
Description	When PPPoE circuit identifier insertion 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 inserted circuit ID contains the following information: MAC address Device ID Port number By default, the Switch IP address is used as the device ID to encode the circuit ID option.
Parameters	*[enable* | *disable]* – Enables or disable PPPoE circuit ID insertion globally. The function is disabled by default.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To globally enable PPPoE circuit identifier insertion:

```
DGS-1210-28MP:5# config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable
```

```
Success.
```

config pppoe circuit_id_insertion ports

Purpose	Used to enable and disable PPPoE circuit identifier insertion on a per port basis and specify how to encode the circuit ID option.
Syntax	**config pppoe circuit_id_insertion ports [all | <portlist >] [circuit_id [mac | ip | udf <string 32>] | state [enable | disable]]**
Description	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, inserted by the system, from the received PPPoE offer and session confirmation packet.
Parameters	*[all | <portlist >]* – Specifies a list of ports or all ports to be configured. The default settings are enabled for ID insertion per port, but disabled globally. *circuit_id* – Configures the device ID used for encoding of the circuit ID option. *mac* – Specifies that the Switch MAC address be used to encode the circuit ID option. *ip* – Specifies that the Switch IP address be used to encode the circuit ID option. *udf* – A user defined string to be used to encode the circuit ID option. The maximum length is 32. The default encoding for the device ID option is the Switch IP address. *state* – Specify to enable or disable PPPoE circuit ID insertion for the ports listed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable port 1 PPPoE circuit ID insertion function and use MAC of switch:

```
DGS-1210-28MP:5# config pppoe circuit_id_insertion ports 1 circuit_id mac
Command: config pppoe circuit_id_insertion ports 1 circuit_id mac


Success.

DGS-1210-28MP:5# config pppoe circuit_id_insertion ports 1 state enable
Command: config pppoe circuit_id_insertion ports 1 state enable


Success.
```

show pppoe circuit_id_insertion

Purpose	Used to display the PPPoE circuit identifier insertion status for the Switch.
Syntax	**show pppoe circuit_id_insertion**
Description	The **show pppoe circuit_id_insertion** command is used to display the global state configuration of the PPPoE circuit ID insertion function.
Parameters	None.
Restrictions	None.

Example usage:

To view the global PPPoE ID insertion state:

```
DGS-1210-28MP:5# show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status : Enabled
```

show pppoe circuit_id_insertion ports

Purpose	Used to display the PPPoE ID insertion configuration on a per port basis.
Syntax	**show pppoe circuit_id_insertion ports {all | <portlist >}**
Description	The **show pppoe circuit_id_insertion ports** command allows the user to view the configuration of PPPoE ID insertion for each port.
Parameters	*{all | <portlist >}* - Specifies which ports to display. If no ports are specified, all ports configuration will be listed.
Restrictions	None.

Example usage:

To view the PPPoE circuit ID configuration for ports 1 to 3:

```
DGS-1210-28MP:5# show pppoe circuit_id_insertion ports 1-3
Command: show pppoe circuit_id_insertion ports 1-3

Port  State      Circuit ID
----- ---------- ---------------------------------------------
1     Enabled    Switch MAC
2     Disabled   Switch IP
3     Disabled   Switch IP
```

9

NETWORK MANAGEMENT (SNMP) COMMANDS

The Switch supports the Simple Network Management Protocol (SNMP) versions 1, 2c, and 3. Users can specify which version of the SNMP users want to use to monitor and control the Switch. The three versions of SNMP vary in the level of security provided between the management station and the network device. The following table lists the security features of the three SNMP versions:

SNMP Version	Authentication Method	Description
v1	Community String	Community String is used for authentication - NoAuthNoPriv
v2c	Community String	Community String is used for authentication - NoAuthNoPriv
v3	Username	Username is used for authentication – NoAuthNoPriv
v3	MD5 or SHA	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthNoPriv
v3	MD5 DES or SHA DES	Authentication is based on the HMAC-MD5 or HMAC-SHA algorithms – AuthPriv. DES 56-bit encryption is added based on the CBC-DES(DES-56) standard

The Network Management commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create snmp user	<username 32> <groupname 32> [v1 | v2c | v3 [MD5 <auth_password 32> | SHA <auth_password 32> | none] [DES <priv_password 32> | none]]
delete snmp user	<username 32> [v1 | v2c | v3]
show snmp user	
create snmp view	<view_name 32> <oid 32> <oid_mask 32 view_type [included | excluded]
delete snmp view	<view_name 32> [all | <oid 32>]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> <username 32>
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID 64>
create snmp group	<groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]{notify_view <view_name 32>}] {read_view <view_name 32> | write_view <view_name 32>}
delete snmp group	<groupname 32> [v1 | v2c | v3] [auth_nopriv | auth_priv | noauth_priv]
show snmp groups	
show snmp global state	
create snmp host	<ipaddr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]

Command	Parameter
delete snmp host	<ipaddr>
show snmp host	{<ipaddr>}
create snmp v6host	<ip6_addr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]
delete snmp v6host	<ip6_addr>
show snmp v6host	<ip6_addr>
config snmp traps	{ address_binding | stp_new_root | stp_topo_change | authenticate | coldstart | warmstart | linkchange | firmware_upgrade | port_security_violation | lbd | duplicate_ip_detected | dos_prevention | flood_fdb | traffic_control | poe_error | poe_onoff | poe_over_budget | all } state [enable | disable]
show snmp traps	
enable snmp authenticate traps	
disable snmp authenticate traps	
config snmp system_location	<string 32>
config snmp system_name	<string 32>
config snmp system_contact	<string 32>
enable snmp	
disable snmp	
enable community_encryption	
disable community_encryption	
show community_encryption	

Each command is listed in detail, as follows:

create snmp user	
Purpose	To create a new SNMP user and add the user to an SNMP group.
Syntax	**create snmp user <username 32> <groupname 32> [v1 | v2c | v3 [MD5 <auth_password 32> | SHA <auth_password 32> | none] [DES <priv_password 32> | none]]**
Description	The **create snmp user** command creates a new SNMP user and adds the user to an existing SNMP group.
Parameters	*<username 32>* − The new SNMP username, up to 32 alphanumeric characters. *<groupname 32>* − The SNMP groupname the new SNMP user is associated with, up to 32 alphanumeric characters.

	auth - The user may also choose the type of authentication algorithms used to authenticate the snmp user. The choices are: • *MD5* − Specifies that the HMAC-MD5-96 authentication level to be used. md5 may be utilized by entering one of the following: • *<auth password 32>* - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • *SHA* − Specifies that the HMAC-SHA-96 authentication level will be used. • *<priv_password 32>* - A string of between 1 and 32 alphanumeric characters used to authorize the agent to receive packets for the host. • *DES* − Specifies that the DES authentication level will be used.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DGS-1210-28MP:5# create snmp user dlink SW22 v3 MD5 1234 DES jklj22
Command: create snmp user dlink SW22 v3 MD5 1234 DES jklj22

Success.
DGS-1210-28MP:5#
```

delete snmp user

Purpose	To remove an SNMP user from an SNMP group and also to delete the associated SNMP group.
Syntax	**delete snmp user <username 32> [v1 | v2c | v3]**
Description	The **delete snmp user** command removes an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	*<username 32>* − A string of up to 32 alphanumeric characters that identifies the SNMP user to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete a previously created SNMP user on the Switch:

```
DGS-1210-28MP:5# delete snmp user dlink v3
Command: delete snmp user dlink v3

Success.
DGS-1210-28MP:5#
```

show snmp user

Purpose	To display information about each SNMP username in the SNMP group username table.
Syntax	**show snmp user**

Description	The **show snmp user** command displays information about each SNMP username in the SNMP group username table.
Parameters	None.
Restrictions	None.

Example usage:

To display the SNMP users currently configured on the Switch:

```
DGS-1210-28MP:5# show snmp user
Command: show snmp user

Username    Group Name    SNMP Version    Auth-Protocol      PrivProtocol
----------  ----------    ------------    --------------     ------------

ReadOnly    ReadOnly      V1              None               None
ReadOnly    ReadOnly      V2              None               None
ReadWrite   ReadWrite     V1              None               None
ReadWrite   ReadWrite     V2              None               None

Total Entries: 4

DGS-1210-28MP:5#
```

create snmp view

Purpose	To assign views to community strings to limit which MIB objects an SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid 32> <oid_mask 32 view_type [included | excluded]**
Description	The **create snmp view** command assigns views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	*<view_name 32>* − A string of up to 30 alphanumeric characters that identifies the SNMP view to be created. *<oid 32>* − The object ID that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. *<oid_mask 32>* − The object ID mask that identifies an object tree (MIB tree) to be included or excluded from access by an SNMP manager. *included* − Includes this object in the list of objects that an SNMP manager can access. *excluded* − Excludes this object from the list of objects that an SNMP manager can access.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP view:

```
DGS-1210-28MP:5# create snmp view dlink 1.3.6 1.1.1 view_type excluded
Command: create snmp view dlink 1.3.6 1.1.1 view_type excluded
```

```
Success.
DGS-1210-28MP:5#
```

delete snmp view

Purpose	To remove an SNMP view entry previously created on the Switch.
Syntax	**delete snmp view <view_name 32> [all | <oid 32>]**
Description	The **delete snmp view** command removes an SNMP view previously created on the Switch.
Parameters	*<view_name 32>* − A string of up to 32 alphanumeric characters that identifies the SNMP view to be deleted. *[all | <oid 32>]* − The object ID that identifies an object tree (MIB tree) that is deleted from the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete all configured SNMP view from the Switch:

```
DGS-1210-28MP:5#  delete snmp view dlink all
Command: delete snmp view dlink all

Success.
DGS-1210-28MP:5#
```

show snmp view

Purpose	To display an SNMP view previously created on the Switch.
Syntax	**show snmp view {<view_name 32>}**
Description	The **show snmp view** command displays an SNMP view previously created on the Switch.
Parameters	*<view_name 32>* − A string of up to 30 alphanumeric characters that identifies the SNMP view to be displayed.
Restrictions	None.

Example usage:

To display SNMP view configuration:

```
DGS-1210-28MP:5# show snmp view
Command: show snmp view

SNMP View Table Configuration
View Name       Subtree OID           OID Mask        View Type
------------    ----------------------  ----------------------  ----------------
dlink           1.2.3.4                 1.1.1.1         Excluded
ReadWrite       1                       1               Included

Total Entries: 2

DGS-1210-28MP:5#
```

create snmp community

Purpose	To create an SNMP community string to define the relationship between the SNMP manager and an SNMP agent.
Syntax	**create snmp community <community_string 32> <username 32>**
Description	The **create snmp community** command creates an SNMP community string and assigns access-limiting characteristics to this community string. The community string acts like a password to permit access to the agent on the Switch. One or more of the following characteristics can be associated with the community string: An Access List of IP addresses of SNMP managers that are permitted to use the community string to gain access to the Switch's SNMP agent. A MIB view that defines the subset of all MIB objects to be accessible to the SNMP community. Read/write or read-only level permission for the MIB objects accessible to the SNMP community.
Parameters	<*community_string 32*> − A string of up to 32 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. <*username 32*> − A string of up to 32 alphanumeric characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create the SNMP community string 'dlink:'

```
DGS-1210-28MP:5# create snmp community dlinkgroup dlink
Command: create snmp community dlinkgroup dlink

Success.

DGS-1210-28MP:5#
```

delete snmp community

Purpose	To remove a specific SNMP community string from the Switch.
Syntax	**delete snmp community <community_string 32>**
Description	The **delete snmp community** command removes a previously defined SNMP community string from the Switch.
Parameters	<*community_string 32*> − A string of up to 32 alphanumeric characters that is used to identify members of an SNMP community to delete. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the SNMP community string 'dlinkgroup':

```
DGS-1210-28MP:5# delete snmp community dlinkgroup
Command: delete snmp community dlinkgroup

Success.
DGS-1210-28MP:5#
```

show snmp community

Purpose	To display SNMP community strings configured on the Switch.
Syntax	**show snmp community {<community_string 32>}**
Description	The **show snmp community** command displays SNMP community strings that are configured on the Switch.
Parameters	*<community_string 32>* − A string of up to 20 alphanumeric characters that is used to identify members of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently entered SNMP community strings:

```
DGS-1210-28MP:5#  show snmp community
Command: show snmp community

SNMP Community Table
(Maximum Entries : 10)
Community Name          User Name
---------------          ----------
private                  ReadWrite
public                   ReadOnly

Total Entries: 2

DGS-1210-28MP:5#
```

config snmp engineID

Purpose	To configure a name for the SNMP engine on the Switch.
Syntax	**config snmp engineID <snmp_engineID 64>**
Description	The **config snmp engineID** command configures a name for the SNMP engine on the Switch.
Parameters	*<snmp_engineID 64>* − A string, of between 10 and 64 alphanumeric characters, to be used to identify the SNMP engine on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To give the SNMP agent on the Switch:

```
DGS-1210-28MP:5# config snmp engineID 12345678900
```

```
Command: config snmp engineID 12345678900

Success.
DGS-1210-28MP:5#
```

show snmp engineID

Purpose	To display SNMP community strings configured on the Switch.
Syntax	**show snmp engineID**
Description	The **show snmp engineID** command displays SNMP engine ID configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently SNMP engine ID:

```
DGS-1210-28MP:5# show snmp engineID
Command: show snmp engineID

Default SNMP Engine ID      : 800000ab03ecade062afa0
SNMP Engine ID              : 1213123123123123123123
```

create snmp group

Purpose	To create a new SNMP group, or a table that maps SNMP users to SNMP views.
Syntax	**create snmp group <groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]{notify_view <view_name 32>}] {read_view <view_name 32> | write_view <view_name 32>}**
Description	The **create snmp group** command creates a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* − A name of up to 30 alphanumeric characters that identifies the SNMP group the new SNMP user is to be associated with. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − Ensures that packets have not been tampered with during transit. • Authentication − Determines if an SNMP message is from a

	valid source. • Encryption − Scrambles the contents of messages to prevent it from being viewed by an unauthorized source. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. • <*view_name 32*> − A string of up to 32 objects that a remote SNMP manager is allowed to access on the Switch. *write_view* – Specifies that the SNMP group being created has write privileges. • <*view_name 32* identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *notify_view* − Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. • <*view_name 32*> − A string of up to 32 alphanumeric characters that identifies the group of MIB objects that a remote SNMP manager is allowed to access on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an SNMP group named 'sg1:'

```
DGS-1210-28MP:5# create snmp group sg1 v2c read_view sg1 write_view sg1 notify_view sg1
Command: create snmp group sg1 v2c read_view sg1 write_view sg1 notify_view sg1

Success.
DGS-1210-28MP:5#
```

delete snmp group

Purpose	To remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32> [v1 | v2c | v3 [auth_priv | noauth_nopriv]]**
Description	The **delete snmp group** command removes an SNMP group from the Switch.
Parameters	<*groupname 32*> − A string of that identifies the SNMP group the new SNMP user will be associated with. Up to 32 alphanumeric characters.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the SNMP group named 'sg1':

```
DGS-1210-28MP:5#  delete snmp group sg1 v2c
Command: delete snmp group sg1 v2c

Success.
DGS-1210-28MP:5#
```

show snmp groups

Purpose	To display the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Syntax	**show snmp groups**
Description	The **show snmp groups** command displays the group-names of SNMP groups currently configured on the Switch. The security model, level, and status of each group are also displayed.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DGS-1210-28MP:5# show snmp groups
Command: show snmp groups

SNMP Group Table
(Maximum Entries : 10)

Group Name  Read View  Write View  Notify View  Security Model   Security Level
----------- ---------- ----------- ------------ ---------------- ---------------
sg1         df         df          d            v3               AuthPriv
ReadOnly    ReadWrite  ---         ReadWrite    v1               NoAuthNoPriv
ReadOnly    ReadWrite  ---         ReadWrite    v2c              NoAuthNoPriv
ReadWrite   ReadWrite  ReadWrite   ReadWrite    v1               NoAuthNoPriv
ReadWrite   ReadWrite  ReadWrite   ReadWrite    v2c              NoAuthNoPriv

Total Entries: 5

DGS-1210-28MP:5#
```

show snmp global state

Purpose	To display the global state of SNMP currently configured on the Switch.
Syntax	**show snmp global state**
Description	The **show snmp global state** command displays the global state of SNMP groups currently configured on the Switch.
Parameters	None.

Restrictions	None.

Example usage:

To display the currently SNMP global state on the Switch:

```
DGS-1210-28MP:5# show snmp global state
Command: show snmp global state

SNMP Global State : Enable

DGS-1210-28MP:5#
```

create snmp host

Purpose	To create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**create snmp host <ipaddr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]**
Description	The **create snmp host** command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* − The IP address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source. • Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − A string of up to 32 alphanumeric characters that identifies user name of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are

	encrypted.
Restrictions	Only Administrator and oper-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-1210-28MP:5# create snmp host 10.90.90.22 v3 noauth_nopriv dlink
Command: create snmp host 10.90.90.22 v3 noauth_nopriv dlink

Success.
DGS-1210-28MP:5#
```

delete snmp host

Purpose	To remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp host <ipaddr>**
Description	The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To delete an SNMP host entry:

```
DGS-1210-28MP:5# delete snmp host 10.90.90.22
Command: delete snmp host 10.90.90.22

Success.
DGS-1210-28MP:5#
```

show snmp host

Purpose	To display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp host {<ipaddr>}**
Description	The **show snmp host** command is used to display the IP addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* − The IP address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently SNMP hosts on the Switch:

```
DGS-1210-28MP:5# show snmp host
Command: show snmp host
```

```
SNMP Host Table
(Maximum Entries : 10)

Host IP Address     SNMP Version      Community Name/SNMPv3 User Name
----------------------- ---------------------  ----------------------------------------------------------
10.90.90.22             V3-NoAuthNoPriv   dlink

Total Entries : 1

DGS-1210-28MP:5#
```

create snmp v6host

Purpose	To create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**create snmp v6host <ip6_addr> [v1 <username 32> | v2c <username 32> | v3 [noauth_nopriv | auth_nopriv | auth_priv] <username 32>]**
Description	The **create snmp v6host** command creates a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipv6_addr>* − The IPv6 address of the remote management station to serve as the SNMP host for the Switch. *v1* – Specifies that SNMP version 1 is to be used. The Simple Network Management Protocol (SNMP), version 1, is a network management protocol that provides a means to monitor and control network devices. *v2c* – Specifies that SNMP version 2c is to be used. The SNMP v2c supports both centralized and distributed network management strategies. It includes improvements in the Structure of Management Information (SMI) and adds some security features. *v3* – Specifies that the SNMP version 3 is to be used. SNMP v3 provides secure access to devices through a combination of authentication and encrypting packets over the network. SNMP v3 adds: • Message integrity − ensures that packets have not been tampered with during transit. • Authentication − determines if an SNMP message is from a valid source. • Encryption − scrambles the contents of messages to prevent it being viewed by an unauthorized source. *<username 32>* − A string of up to 32 alphanumeric characters that identifies user name of an SNMP community. This string is used like a password to give remote SNMP managers access to MIB objects in the Switch's SNMP agent. *noauth_nopriv* − Specifies that there is no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* − Specifies that authorization is required, but there is no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* − Specifies that authorization is required, and that packets sent between the Switch and a remote SNMP manger are

	encrypted.
Restrictions	Only Administrator and oper-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-1210-28MP:5# create snmp v6host 3000::1 v3 noauth_nopriv dlink
Command: create snmp v6host 3000::1 v3 noauth_nopriv dlink

Success.
DGS-1210-28MP:5#
```

delete snmp v6host

Purpose	To remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp v6host <ip6_addr>**
Description	The **delete snmp host** command deletes a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<*ipv6_addr*> − The IPv6 address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To delete an SNMP IPv6 host entry:

```
DGS-1210-28MP:5# delete snmp v6host 3000::1
Command: delete snmp v6host 3000::1


Success.
```

show snmp v6host

Purpose	To display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp v6host {<ip6_addr>}**
Description	The **show snmp host** command is used to display the IPv6 addresses and configuration information of remote SNMP managers that are designated as recipients of SNMP traps generated by the Switch's SNMP agent.
Parameters	<*ip6_addr*> − The IPv6 address of a remote SNMP manager that receives SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DGS-1210-28MP:5# show snmp v6host
Command: show snmp v6host
```

```
SNMP Host Table
(Maximum Entries : 10)

Host IP Address                 SNMP Version      Community or User Name
---------------------------------- ------------------- ----------------------------------
3000::1                         V3-NoAuthNoPriv   dlink

Success.
DGS-1210-28MP:5#
```

config snmp traps

Purpose	To configure SNMP traps in supported events.
Syntax	**config snmp traps { address_binding | stp_new_root | stp_topo_change | authenticate | coldstart | warmstart | linkchange | firmware_upgrade | port_security_violation | lbd | duplicate_ip_detected | dos_prevention | flood_fdb | traffic_control | poe_error | poe_onoff | poe_over_budget | all } state [enable | disable]**
Description	The **config snmp traps** command enables SNMP trap support on the Switch.
Parameters	*address_binding* – Adress binding function related traps *stp_new_root* – Traps when new STP root selected *stp_topo_change* – Traps when STP topology changed *authentication* – Traps for authentication failure *coldstart* – Trap for system coldstart event *warmstart* – Trap for system warmstart event *linkchange* – Trap for link change event *firmware_upgrade* – Trap for status of firmware upgrade process *port_security_violation* – Traps for port security violation event *lbd* – Loopback detection function related traps *duplicate_ip_detection* – Trap for duplicate IP detected event *dos_prvention* – DoS prevention function related traps *flood_fdb* – Trap for flood fdb function *traffic_control* – Traffic control function related traps *poe_error* – Trap for error occurred in PoE *poe_onoff* – Trap for port PoE state *poe_over_budget* – Trap for over budget event in PoE *all* – All the feature listed
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To configure SNMP trap feature on the Switch:

```
DGS-1210-10MP:5# config snmp traps all state enable
Command: config snmp traps all state enable
```

```
Success.

DGS-1210-10MP:5#
```

show snmp traps

Purpose	To display SNMP trap support status on the Switch.
Syntax	**show snmp traps**
Description	The **show snmp traps** command displays the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DGS-1210-10MP:5# show snmp traps
Command: show snmp traps

SNMP Authentication Traps          : Enabled
Coldstart Traps                    : Enabled
Warmstart Traps                    : Enabled
Linkchange Traps                   : Enabled on ports 1-10
STP New Root Traps                 : Enabled
STP Topology Change Traps          : Enabled
Firmware Upgrade State Traps       : Enabled
Port Security violation Traps      : Enabled
Loopback detection Traps           : Enabled
Traffic control Traps              : Storm Occurred and Storm
Cleared
DoS Prevention violation Traps     : Enabled
Duplicate IP Detected Traps        : Enabled
address_binding Traps              : Enabled
flood_fdb Traps                    : Enabled
PoE Power On/Off Traps             : Enabled
PoE Power Error Traps              : Enabled
over max power budget Traps        : Enabled

DGS-1210-10MP:5#
```

config snmp system_location

Purpose	To enter a description of the location of the Switch.
Syntax	**config snmp sysem_location <string 32>**
Description	The **config syslocation** command enters a description of the location of the Switch. A maximum of 32 characters can be used.
Parameters	*<string 32>* - A maximum of 32 characters is allowed.

Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch location for 'HQ5F':

```
DGS-1210-28MP:5# config snmp system_location HQ5F
Command: config snmp system_location HQ5F

Success.
DGS-1210-28MP:5#
```

config snmp system_name

Purpose	To define the name for the Switch.
Syntax	**config snmp system_name <string 32>**
Description	The **config snmp system_name** command defines the name of the Switch.
Parameters	<*string 32*> - A maximum of 32 characters is allowed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch name:

```
DGS-1210-28MP:5# config snmp system_name DLINK_switch
Command: config snmp system_name DLINK_switch

Success.
DGS-1210-28MP:5#
```

config snmp system_contact

Purpose	To define the name for the Switch.
Syntax	**config snmp system_contact <string 32>**
Description	The **config snmp system_contact** command is used to configure the contact information presented in swtch information.
Parameters	<*string 32*> - A maximum of 32 characters is allowed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch contact name:

```
DGS-1210-28MP:5# config snmp system_contact DLINK_support
Command: config snmp system_contact DLINK_support

Success.
DGS-1210-28MP:5#
```

enable snmp

Purpose	To enable SNMP support.
Syntax	**enable snmp**
Description	The **enable snmp** command enables SNMP support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP support on the Switch:

```
DGS-1210-28MP:5# enable snmp
Command: enable snmp

Success.
DGS-1210-28MP:5#
```

disable snmp

Purpose	To disable SNMP support.
Syntax	**disable snmp**
Description	The **disable snmp** command enables SNMP support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP support on the Switch:

```
DGS-1210-28MP:5# disable snmp
Command: disable snmp

Success.
DGS-1210-28MP:5#
```

enable community_encryption

Purpose	To enable encryption mechanism of SNMP community string.
Syntax	**enable community_encryption**
Description	The **enable community_encryption** command enables the mechanism to encryption SNMP community string which provides higher security level for user.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To enable encryption of SNMP community string:

```
DGS-1210-28MP:5# enable community_encryption
Command: enable community_encryption
```

```
Success.
```

disable community_encryption

Purpose	To disable encryption mechanism of SNMP community string.
Syntax	**disable community_encryption**
Description	The **disable community_encryption** command disables the mechanism of encryption SNMP community string.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To disable encryption of SNMP community string:

```
DGS-1210-28MP:5# disable community_encryption
Command: disable community_encryption


Success.
```

show community_encryption

Purpose	To display cureent encryption mechanism state of SNMP community string.
Syntax	**show community_encryption**
Description	The **show community_encryption** command disables the mechanism of encryption SNMP community string.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To display current state of SNMP community encryption:

```
DGS-1210-28MP:5# show community_encryption
Command: show community_encryption


SNMP Community Encryption State : Disabled


DGS-1210-28MP:5#
```

10

DOWNLOAD/UPLOAD COMMANDS

The Download/Upload commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
download	[cfg_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [firmware_fromTFTP [<ipaddr> | <ipv6_addr>] < path_filename 64>] | [log_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [log_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>]
upload	[[firmware_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [cfg_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>]

Each command is listed in detail, as follows:

download	
Purpose	To download and install a firmware, boot, or switch configuration file from a TFTP server.
Syntax	**download [cfg_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [firmware_fromTFTP [<ipaddr> | <ipv6_addr>] < path_filename 64>] | [log_fromTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [log_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>]**
Description	The **download** command downloads a firmware, boot, log or switch configuration file from a TFTP server.
Parameters	*cfg_fromTFTP* − Downloads a switch configuration file from a TFTP server. <*ipaddr*> − The IPv4 address of the TFTP server. <*ipv6_addr*> − The IPv6 address of the TFTP server. <*path_filename 64*> − The DOS path and filename of the switch configuration file, up to 64 characters, on the TFTP server. For example, C:\31xx.had. *startup* − Indicates the Configuration file is to be downloaded to the startup config. *firmware_fromTFTP* − Downloads and installs firmware on the Switch from a TFTP server. < *path_filename 64*> − The DOS path and filename of the firmware file or log file, up to 64 characters, on the TFTP server. For example, C:\31xx.had. *log_fromTFTP* − Downloads a log file from a TFTP server. *cfg_toTFTP* − Downloads a log file to a TFTP server.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To download a firmware file:

```
DGS-1210-28MP:5#  download  firmware_fromTFTP  10.90.90.123  DGS-1210-
```

```
SERIES-2-00-00
5-ALL.hex
Command: download firmware_fromTFTP 10.90.90.123 DGS-1210-SERIES-2-00-005-ALL.hex

Connecting to Server.....  Done
Transfer firmware.....  Done
Upgrade processing.....  Done
Firmware upgrade successfully!


Success.

DGS-1210-28MP:5#
```

To download a configuration file:

```
DGS-1210-28MP:5# download cfg_fromTFTP 10.90.90.123 test.cfg
Command: download cfg_fromTFTP 10.90.90.123 test.cfg

Connecting to server.....  Done
Transfer configuration.....  Done. Do not power off!!
Config restore successfully!

Success.
```

upload

Purpose	To upload the current switch settings to a TFTP server.
Syntax	**upload [[firmware_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [cfg_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>**
Description	The **upload** command uploads the Switch's current settings to a TFTP server.
Parameters	*firmware_toTFTP* − Specifies that the Switch's current firmware are to be uploaded to the TFTP server. *<ipaddr>* − The IPv4 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. *<ipv6_addr>* − The IPv6 address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. *<path_filename 64>* − The location of the Switch configuration file on the TFTP server. *cfg_fromTFTP* − Uploads a switch configuration file from a TFTP server.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

```
DGS-1210-28MP:5# upload cfg_toTFTP 10.90.90.123 test.cfg
Command: upload cfg_toTFTP 10.90.90.123 test.cfg
```

```
Connecting to server.....    Done
Transfer configuration.....    Done. Do not power off!!
Config backup  successfully!

Success.
```

11

DHCP RELAY COMMANDS

The DHCP Relay commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable dhcp_relay	
disable dhcp_relay	
config dhcp_relay add ipif system	<ipaddr>
config dhcp_relay delete ipif system	<ipaddr>
config dhcp_relay hops	<value 1-16>
config dhcp_relay option_82	[check [enable | disable] | policy [drop | keep | replace] | remote_id [default | user_define <string 32>] | state [enable | disable]]
show dhcp_relay	{ipif}
enable dhcp_local_relay	
disable dhcp_local_relay	
config dhcp_local_relay	vlan [<vlan_name 20> | vlanid <vidlist>] state[enable | disable]
show dhcp_local_relay	
enable dhcpv6_relay	
disable dhcpv6_relay	
show dhcpv6_relay	{ipif system}
config dhcpv6_relay	[add | delete] ipif System <ipv6_addr>
config dhcpv6_relay hop_count	<value 1-32>
Config dhcpv6_relay option_37	[state [enable | disable]| check] [enable | disable] | remote_id [default | cid_with_user_define <string 128> | user_define <string 128>]]

Each command is listed in detail, as follows:

enable dhcp_relay	
Purpose	To enable DHCP Relay server on the Switch
Syntax	**enable dhcp_relay**
Description	The **enable dhcp_relay** command sets the DHCP Relay to be globally enabled on the Switch and on all existing VLANs.

Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To enable DHCP Relay on the Switch:

```
DGS-1210-28MP:5# enable dhcp_relay
Command: enable dhcp_relay

Success.
DGS-1210-28MP:5#
```

disable dhcp_relay

Purpose	To disable DHCP Relay server on the Switch
Syntax	**disable dhcp_relay**
Description	The **disable dhcp_relay** command sets the DHCP Relay to be globally disabled on the Switch and on all existing VLANs.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable DHCP Relay on the Switch:

```
DGS-1210-28MP:5# disable dhcp_relay
Command: disable dhcp_relay

Success.
DGS-1210-28MP:5#
```

config dhcp_relay add ipif System

Purpose	To define a DHCP server as a DHCP Relay server
Syntax	**config dhcp_relay add ipif System <ipaddr>**
Description	The **config dhcp_relay add ipif System** command adds DHCP servers as DHCP Relay servers.
Parameters	*<ipaddr>* − The IP address of the DHCP server. Up to 4 servers can be defined.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To add a DHCP server as a DHCP Relay server:

```
DGS-1210-28MP:5# config dhcp_relay add ipif System 10.6.150.49
Command: config dhcp_relay add ipif System 10.6.150.49

Success.
DGS-1210-28MP:5#
```

config dhcp_relay delete ipif System

Purpose	To delete a DHCP server from the DHCP Relay server list.
Syntax	**config dhcp_relay delete ipif System <ipaddr>**
Description	The **config dhcp_relay delete ipif System** command deletes a DHCP servers defined as a DHCP Relay server.
Parameters	*<ipaddr>* − The IP address of the DHCP server.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To remove a DHCP server from the DHCP Relay server list:

```
DGS-1210-28MP:5# config dhcp_relay delete ipif System 10.6.150.49
Command: config dhcp_relay delete ipif System 10.6.150.49

Success.
DGS-1210-28MP:5#
```

config dhcp_relay hops

Purpose	To delete a DHCP server from the DHCP Relay server list.
Syntax	**config dhcp_relay hops <value 1-16>**
Description	The **config dhcp_relay hops** command configures the DHCP/BOOTP relay feature.
Parameters	*<value 1-16>* − Specifies the maximum number of relay agent hops that the DHCP packets can cross.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP relay on the Switch:

```
DGS-1210-28MP:5# config dhcp_relay hops 12
Command: config dhcp_relay hops 12

Success.
DGS-1210-28MP:5#
```

config dhcp_relay option_82

Purpose	To configure the check, policy and state of DHCP relay agent information option 82 of the Switch.
Syntax	**config dhcp_relay option_82 [check [enable | disable] | policy [drop | keep | replace] | remote_id [default | user_define <string 32>] | state [enable | disable]]**
Description	The **config dhcp_relay option_82** is used to configure the check, policy and state of DHCP relay agent information option 82 of the Switch
Parameters	*check:* used to configure the check of DHCP relay agent information option 82 of the Switch. *enable* – When the field is toggled to enable, the relay agent will check the validity of the packet's option 82 field. If the switch

	receives a packet that contains the option 82 field from a DHCP client, the switch drops the packet because it is invalid. In packets received from DHCP servers, the relay agent will drop invalid messages. *disable* – When the field is toggled to disable, the relay agent will not check the validity of the packet's option 82 field. policy: used to configure the re-forwarding policy of DHCP relay agent information option 82 of the Switch. *replace* − The option 82 field will be replaced if the option 82 field already exists in the packet received from the DHCP client. *drop* − The packet will be dropped if the option 82 field already exists in the packet received from the DHCP client. *keep* − The option 82 field will be retained if the option 82 field already exists in the packet received from the DHCP client. state: used to configure the state of DHCP relay agent information option 82 of the Switch. *enable* − When this field is toggled to Enabled the relay agent will insert and remove DHCP relay information (option 82 field) in messages between DHCP server and client. When the relay agent receives the DHCP request, it adds the option 82 information, and the IP address of the relay agent (if the relay agent is configured), to the packet. Once the option 82 information has been added to the packet it is sent on to the DHCP server. When the DHCP server receives the packet, if the server is capable of option 82, it can implement policies like restricting the number of IP addresses that can be assigned to a single remote ID or circuit ID. Then the DHCP server echoes the option 82 field in the DHCP reply. The DHCP server unicasts the reply to the back to the relay agent if the request was relayed to the server by the relay agent. The switch verifies that it originally inserted the option 82 data. Finally, the relay agent removes the option 82 field and forwards the packet to the switch port that connects to the DHCP client that sent the DHCP request. *disable* − If the field is toggled to disable the relay agent will not insert and remove DHCP relay information (option 82 field) in messages between DHCP servers and clients, and the check and policy settings will have no effect.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable the DHCP relay option 82 on the Switch:

```
DGS-1210-28MP:5# config dhcp_relay option_82 state disable
Command: config dhcp_relay option_82 state disable

Success.
DGS-1210-28MP:5#
```

show dhcp_relay

Purpose	To display the DHCP Relay settings on the Switch.
Syntax	**show dhcp_relay {ipif}**

Description	The **show dhcp_relay** command displays the DHCP Relay status and list of servers defined as DHCP Relay servers on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCP Relay settings:

```
DGS-1210-28MP:5# show dhcp_relay
Command: show dhcp_relay

DHCP Relay Status                          : Disabled
DHCP Relay Hops Count Limit                : 4
DHCP Relay Time Threshold                  : 0
DHCP Relay VID List                        : None
DHCP Relay PortList                        : None
DHCP Relay Agent Information Option82 State     : Enabled
DHCP Relay Agent Information Option82 Check     : Disabled
DHCP Relay Agent Information Option82 Policy    : replace
DHCP Relay Agent Information Option82 Remote ID : EC-AD-E0-62-AF-A0

Interface  Server 1       Server 2       Server 3       Server 4
---------  -------------- -------------- -------------- --------------

DGS-1210-28MP:5#
```

enable dhcp_local_relay

Purpose	To enable the DHCP local relay feature globally
Syntax	**enable dhcp_local_relay**
Description	The **enable dhcp_local_relay** command enables the DHCP local relay feature on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the DHCP Local Relay:

```
DGS-1210-28MP:5# enable dhcp_local_relay
Command: enable dhcp_local_relay

Success
DGS-1210-28MP:5#
```

disable dhcp_local_relay

Purpose	To disable the DHCP local relay feature globally
Syntax	**disable dhcp_local_relay**

Description	The **disable dhcp_local_relay** command disables the DHCP local relay feature on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the DHCP Local Relay:

```
DGS-1210-28MP:5# disable dhcp_local_relay
Command: disable dhcp_local_relay

Success.
DGS-1210-28MP:5#
```

config dhcp_local_relay

Purpose	To specify which VLAN's the feature works on.
Syntax	**config dhcp_local_relay vlan [<vlan_name 20> | vlanid <vidlist>] state[enable | disable]**
Description	Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.
Parameters	*<vlan_name 20>* – the VLAN name identifier *vlanid <vidlist>* – The VLAN tag identifier *state [enable | disable]* – enable or disable of the DHCP Local Relay status by VLAN name or VLAN ID.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the VLAN ID10 from VLAN of DHCP Local Relay:

```
DGS-1210-28MP:5# config dhcp_local_relay vlan vlanid 10 state disable
Command: config dhcp_local_relay vlan vlanid 10 state disable


Success.
DGS-1210-28MP:5#
```

show dhcp_local_relay

Purpose	To display which VLAN's the feature works on.
Syntax	**show dhcp_local_relay**
Description	Each VLAN which was added to the DHCP Local Relay list participates in the DHCP Local Relay process – Option 82 is added to DHCP requests on this VLAN, and Removed from DHCP Replies on this VLAN.
Parameters	None.

Restrictions	None.

Example usage:

To display the DHCP local relay information on the Switch:

```
DGS-1210-28MP:5#  show dhcp_local_relay
Command: show dhcp_local_relay

DHCP Local Relay Status        : Disabled
DHCP Local Relay VID List      : 1
DGS-1210-28MP:5#
```

enable dhcpv6_relay

Purpose	To enable DHCPv6 Relay function on the Switch
Syntax	**enable dhcpv6_relay**
Description	The **enable dhcpv6_relay** command is used to enable the DHCPv6 relay global state on the Switch.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To enable DCHPv6 Relay on the Switch:

```
DGS-1210-28MP:5# enable dhcpc6_relay
Command: enable dhcpc6_relay

Success.
DGS-1210-28MP:5#
```

disable dhcp6_relay

Purpose	To disable DHCPv6 Relay function on the Switch
Syntax	**disable dhcpv6_relay**
Description	The **disable dhcpv6_relay** command is used to disable the DHCPv6 relay global state on the Switch.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To disable DHCPv6 Relay on the Switch:

```
DGS-1210-28MP:5# disable dhcpv6_relay
Command: disable dhcpv6_relay

Success.
DGS-1210-28MP:5#
```

show dhcpv6_relay

Purpose	To display the current DHCPv6 relay configuration.
Syntax	**show dhcpv6_relay {ipif system}**
Description	The **show dhcpv6_relay** command displays 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	None.
Restrictions	None.

Example usage:

To display DHCPv6 Relay settings:

```
DGS-1210-28MP:5# show dhcpv6_relay
Command: show dhcpv6_relay

DHCPv6 Relay Status             : Disabled
DHCPv6 Relay Hops Count Limit   : 4
DHCPv6 Relay Option37 State     : Disabled
DHCPv6 Relay Option37 Check     : Disabled
DHCPv6 Relay Option37 Remote ID : EC-AD-E0-62-AF-A0
-------------------------------------------
Interface       Server Address
--------------- ---------------
DGS-1210-28MP:5#
```

config dhcpv6_relay

Purpose	Used to add or delete a destination IP address to or from the switch's DHCPv6 relay table.
Syntax	**config dhcpv6_relay [add | delete] ipif System <ipv6_addr>**
Description	The **config dhcpv6_relay** command can add or delete an IPv6 destination address to forward (relay) DHCPv6 packets.
Parameters	*add* − Add an IPv6 destination to the DHCPv6 relay table. *delete* − Remove an IPv6 destination to the DHCPv6 relay table. *ipif system* − The name of the IP interface in which DHCPv6 relay is to be enabled. <*ipv6_addr*> − The DHCPv6 server IP address.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To add the DHCPv6 relay on the Switch:

```
DGS-1210-28MP:5# config dhcpv6_relay add ipif System 3000::1
Command: config dhcpv6_relay add ipif System 3000::1

Success.
DGS-1210-28MP:5#
```

config dhcpv6_relay hop_count	
Purpose	Used to configure the DHCPv6 relay hop count of the switch.
Syntax	**config dhcpv6_relay hop_count <value 1-32>**
Description	The **config dhcpv6_relay hops_count** command is used to configure the DHCPv6 relay hop count of the switch.
Parameters	*<value 1-32>* − The hop count is the number of relay agents that have to be relayed in this message. The range is 1 to 32. The default value is 4.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay hop count on the Switch:

```
DGS-1210-28MP:5# config dhcpv6_relay hop_count 3
Command: config dhcpv6_relay hop_count 3

Success.
DGS-1210-28MP:5#
```

config dhcpv6_relay option_37	
Purpose	Used to configure the DHCPv6 relay option 37 of the switch.
Syntax	**config dhcpv6_relay option_37 [state [enable | disable]| check] [enable | disable] | remote_id [default | cid_with_user_define <string 128> | user_define <string 128>]]**
Description	The **config dhcpv6_relay hops_count** command is used to configure the DHCPv6 Relay option 37 function.When DHCPv6 relay option 37 is enabled, the DHCP packet is inserted with the option 37 field before being relayed to the server. The DHCP packet will be processed based on the behavior defined in the check and remote ID type setting. When the state is disabled, the DHCP packet is relayed directly to the server.
Parameters	*state [enable | disable]* - Specify DHCPv6 relay option37 state. When the state is enabled, the DHCP packet is inserted with the option 37 field before being relayed to the server. When the state is disabled, the DHCP packet is relayed directly to the server. *check [enable | disable]* - Specify to check the packets or not. When the check state is enabled, packets from client side should not have the option 37 field. If client originating packets have the option 37 field, they will be dropped. Specify for not checking the packets. *remote_id [default | cid_with_user_define <string 128> | user_define <string 128>]* - Specify the content in the remote ID. default – Specify to have the remote ID as VLAN ID + Module + Port +System MAC address of the device. cid_with_user_define – Specify to have the remote ID as VLAN ID + Module + Port + user defined string. user_define – Use the user-defined string as the remote ID.
Restrictions	Only Administrator or operate-level users can issue this command.

Example usage:

To configure the DHCPv6 relay hop count on the Switch:

```
DGS-1210-28MP:5# config dhcpv6_relay hop_count 3
Command: config dhcpv6_relay hop_count 3

Success.
DGS-1210-28MP:5#
```

12

NETWORK MONITORING COMMANDS

The Network Monitoring commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
show packet ports	<portlist >
show statistics ports	<portlist>
show error ports	<portlist >
show utilization	[ports {<portlist>} | cpu | mem]
clear counters ports	<porlist >
clear log	
show log	{[index <value 1-500> - <value 1-500>] | severity [debug | informational | warning]}
save log	
enable syslog	
disable syslog	
create syslog host	<index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [informational | warning | debug] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>]}
config syslog host	[all | <index 1-4>] {severity [informational | warning | debug] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>] | ipaddress [<ipaddr> | <ipv6addr>]}
delete syslog host	[<index 1-4> | all]
show syslog host	{<index 1-4>}
cable diagnostic port	[<portlist > | all]

Each command is listed in detail, as follows:

show packet ports	
Purpose	To display statistics about the packets sent and received in frames per second by the Switch.
Syntax	**show packet ports <portlist >**
Description	The **show packet ports** command displays statistics about packets sent and received by ports specified in the port list. The results are separated into three tables, labeled A, B, and C in the window below. Table A is relevant to the size of the packets, Table B is relevant to the type of packets and Table C is relevant to the type of frame associated with these packets.

Parameters	*<portlist >* − A port or range of ports whose statistics are to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 5:

```
DGS-1210-28MP:5# show packet ports 5
Command: show packet ports

 Port Number : 1
 Frame Size   Frame Counts  Frames/sec   Frame Type   Total    Total/sec
 ----------- ------------- ------------ ------------ --------- ----------
 64           2161          2           RX Bytes     168377    128
 65-127       249           0           RX Frames    2435       2
 128-255      18            0
 256-511      7             0           TX Bytes     331492    1071
 512-1023     0             0           TX Frames    3550       3
 1024-1518    0             0

 Unicast RX   2158          2
 Multicast RX 5             0
 Broadcast RX 272           0

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

show statistics ports

Purpose	To display the packet type statistics for a port or a range of ports.
Syntax	**show statistics ports <portlist >**
Description	The **show statistics ports** command displays the packet statistics in packet type basis.
Parameters	*<portlist >* − A port or range of ports whose error statistics are to be displayed.
Restrictions	None.

Example usage:

To display the statistics of port 5:

```
DGS-1210-28MP:5# show statistics ports 5
Command: show statistics ports 5

Port Number : 5
----------------
                TX                      RX
OutOctets       6509619     InOctets        16169750
OutUcastPkts    11486       InUcastPkts     11141
OutNUcastPkts   72676       InNUcastPkts    12101
OutErrors       0           InDiscards      12071
LateCollisions  0           InErrors        0
```

```
ExcessiveCollisions      0          FCSErrors          0
                                    FrameTooLongs      0

DGS-1210-28MP:5#
```

show error ports

Purpose	To display the error statistics for a port or a range of ports.
Syntax	**show error ports <portlist >**
Description	The **show error ports** command displays all of the packet error statistics collected and logged by the Switch for a given port list.
Parameters	*<portlist >* − A port or range of ports whose error statistics are to be displayed.
Restrictions	None.

Example usage:

To display the errors of port 1:

```
DGS-1210-28MP:5# show errors port 1
Command: show error ports 1


Port Number : 1
                RX Frames                       TX Frames
---------------                 -------------------
CRC Error       0               Excessive Deferral  0
Undersize       0               CRC Error           0
Oversize        0               Late Collision      0
Fragment        8               Excessive Collision 0
Jabber          0               Single Collision    0
Drop Pkts       0               Collision           0

DGS-1210-28MP:5#
```

show utilization

Purpose	To display real-time port utilization statistics.
Syntax	**show utilization [ports {<portlist >} | cpu | dram]**
Description	The **show utilization** command displays the real-time utilization statistics for ports in bits per second (bps) for the Switch, and for the CPU in percentage..
Parameters	*ports{* – Entering this parameter will display the current port utilization of the Switch. *<portlist >* – Specifies a range of ports to be displayed. *cpu* – Entering this parameter will display the current CPU utilization of the Switch. *dram* – Entering this parameter will display the current memory utilization of the Switch.
Restrictions	None.

To display the port utilization statistics:

```
DGS-1210-28MP:5# show utilization ports 5
Command: show utilization ports 5



Port      TX Pkts/sec  RX Pkts/sec  Util
----      -----------  -----------  ----
5          1            0            0
```

To display the cpu utilization statistics:

```
DGS-1210-28MP:5# show utilization cpu
Command: show utilization cpu



CPU Utilization:
-------------------------------------------------------------------------------
Five Seconds: 1  %
One  Minute : 1  %
Five Minute : 2  %
```

clear counters

Purpose	To clear the Switch's statistics counters.
Syntax	**clear counters ports <porlist >**
Description	The **clear counters** command clears the counters used by the Switch to compile statistics.
Parameters	*<portlist >* – Specifies a range of ports to be cleared.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-1210-28MP:5#  clear counters ports 2-5
Command: clear counters ports 2-5

Success.
DGS-1210-28MP:5#
```

clear log

Purpose	To clear the Switch's history log.
Syntax	**clear log**
Description	The **clear log** command clears the Switch's history log.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To clear the log information:

```
DGS-1210-28MP:5# clear log
Command: clear log

Success.
DGS-1210-28MP:5#
```

show log

Purpose	To display the Switch history log.
Syntax	**show log {[index <value 1-500> - <value 1-500>] | severity [debug | informational | warning]}**
Description	The **show log** command displays the contents of the Switch's history log.
Parameters	*index <value 1-500>* − The number of entries in the history log to display. *severity [debug | informational | warning]* − Specifies the severity type to be displayed.
Restrictions	None.

Example usage:

To display the Switch history log:

```
DGS-1210-28MP:5# show log
Command: show log


Index Time           Log Text                                        Log Severity
----- ---------------- ---------------------------------------------  ------------
8    Jan  2 05:59:30  [SYSTEM]:Configuration successfully restor      Information
                      ed.
7    Jan  2 05:58:48  [SYSTEM]:Configuration successfully backup      Information
6    Jan  2 05:57:17  [SYSTEM]:Firmware upgraded successfully.        Information
5    Jan  2 02:05:41  [WEB]:Successful login through Web(IP: 10.      Information
                      90.90.123)
4    Jan  2 02:04:45  [LinkStatus]:Port 5 link up, 1Gbps FULL du      Information
                      plex
3    Jan  1 23:29:52  [LinkStatus]:Port 5 link down                   Information
2    Jan  1 06:40:04  [LinkStatus]:Port 5 link up, 1Gbps FULL du      Information
                      plex
1    Jan  1 06:40:04  [SYSTEM]:System started up                      Critical
```

save log

Purpose	To save the Switch history log.
Syntax	**save log**
Description	The **save log** command saves the contents of the Switch's history

	log.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To save the Switch history log:

```
DGS-1210-28MP:5#  save log
Command: save log

Success.
DGS-1210-28MP:5#
```

enable syslog

Purpose	To enable the system log to be sent to a remote host.
Syntax	**enable syslog**
Description	The **enable syslog** command enables the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the syslog function on the Switch:

```
DGS-1210-28MP:5# enable syslog
Command: enable syslog

Success.
DGS-1210-28MP:5#
```

disable syslog

Purpose	To disable the system log from being sent to a remote host.
Syntax	**disable syslog**
Description	The **disable syslog** command disables the system log from being sent to a remote host.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DGS-1210-28MP:5# disable syslog
Command: disable syslog

Success.
DGS-1210-28MP:5#
```

create syslog host

Purpose	To create a new syslog host.
Syntax	**create syslog host <index 1-4> ipaddress [<ipaddr> | <ipv6addr>] {severity [informational | warning | debug] | facility [local0 | local1| local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>]}**
Description	The **create syslog host** command creates a new syslog host.
Parameters	*all* − Specifies that the command is to be applied to all hosts. *<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *ipaddress [<ipaddr> | <ipv6addr>]* − The IPv4 or IPv6 address of the remote host to which syslog messages are to be sent. *severity* − The message severity level indicator. These are described in the table below (Bold font indicates that the corresponding severity level is currently supported on the Switch):

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	**Warning: warning conditions**
5	Notice: normal but significant condition
6	**Informational: informational messages**
7	Debug: debug-level messages

informational − Specifies that informational messages are to be sent to the remote host. This corresponds to number 6 from the list above.

warning − Specifies that warning messages are to be sent to the remote host. This corresponds to number 4 from the list above.

debug − Specifies that debug message are to be sent to the remote host.

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 table below (Bold font indicates the facility values that the Switch currently supports):

Numerical Code	Facility
0	kernel messages
1	user-level messages
2	mail system

	3	system daemons
	4	security/authorization messages
	5	messages generated internally by syslog
	6	line printer subsystem
	7	network news subsystem
	8	UUCP subsystem
	9	clock daemon
	10	security/authorization messages
	11	FTP daemon
	12	NTP subsystem
	13	log audit
	14	log alert
	15	clock daemon
	16	local use 0 (local0)
	17	local use 1 (local1)
	18	local use 2 (local2)
	19	local use 3 (local3)
	20	local use 4 (local4)
	21	local use 5 (local5)
	22	local use 6 (local6)
	23	local use 7 (local7)
	local0 − Specifies that local use 0 messages are to be sent to the remote host. This corresponds to number 16 from the list above.	
	local1 − Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.	
	local2 − Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.	
	local3 − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.	
	local4 − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.	
	local5 − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.	
	local6 − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.	
	local7 − Specifies that local use 7 messages is sent to the remote host. This corresponds to number 23 from the list above.	
	udp_port [514 | <udp_port_number 6000-65535>] − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.	
	state [enable | disable] − Allows the sending of syslog messages to the remote host, specified above, to be enabled and disabled.	
Restrictions	Only Administrator or operator-level users can issue this command.	

Example usage:

To create syslog host:

DGS-1210-28MP:5# create syslog host 1 ipaddress 1.1.2.1 severity informational facility local0 state enable

Command: create syslog host 1 ipaddress 1.1.2.1 severity informational facility

```
local0 state enable

Success.
DGS-1210-28MP:5#
```

config syslog host

Purpose	To configure the syslog protocol to send system log data to a remote host.
Syntax	**config syslog host [all | <index 1-4>] {severity [informational | warning | debug] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | state [enable | disable] | udp_port [514 | <udp_port_number 6000-65535>] | ipaddress [<ipaddr> | <ipv6addr>]}**
Description	The **config syslog host** command configures the syslog protocol to send system log information to a remote host.
Parameters	*all* − Specifies that the command applies to all hosts. *<index 1-4>* − Specifies that the command applies to an index of hosts. There are four available indices, numbered 1 to 4. *severity* − The message severity level indicator. These are described in the following table (Bold font indicates that the corresponding severity level is currently supported on the Switch):

Numerical Code	Severity
0	Emergency: system is unusable
1	Alert: action must be taken immediately
2	Critical: critical conditions
3	Error: error conditions
4	**Warning: warning conditions**
5	Notice: normal but significant condition
6	**Informational: informational messages**
7	Debug: debug-level messages

informational − Specifies that informational messages are to be sent to the remote host. This corresponds to number 6 from the list above.

warning − Specifies that warning messages are to be sent to the remote host. This corresponds to number 4 from the list above.

debug − Specifies that debug message are to be sent to the remote host.

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 indicates the facility values that the Switch currently supports.

Numerical	Facility

Code	
0	kernel messages
1	user-level messages
2	mail system
3	system daemons
4	security/authorization messages
5	messages generated internally by syslog
6	line printer subsystem
7	network news subsystem
8	UUCP subsystem
9	clock daemon
10	security/authorization messages
11	FTP daemon
12	NTP subsystem
13	log audit
14	log alert
15	clock daemon
16	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	local use 7 (local7)

local0 − Specifies that local use 0 messages are to be sent to the remote host. This corresponds to number 16 from the list above.

local1 − Specifies that local use 1 messages are to be sent to the remote host. This corresponds to number 17 from the list above.

local2 − Specifies that local use 2 messages are to be sent to the remote host. This corresponds to number 18 from the list above.

local3 − Specifies that local use 3 messages are to be sent to the remote host. This corresponds to number 19 from the list above.

local4 − Specifies that local use 4 messages are to be sent to the remote host. This corresponds to number 20 from the list above.

local5 − Specifies that local use 5 messages are to be sent to the remote host. This corresponds to number 21 from the list above.

local6 − Specifies that local use 6 messages are to be sent to the remote host. This corresponds to number 22 from the list above.

local7 − Specifies that local use 7 messages are to be sent to the remote host. This corresponds to number 23 from the list above.

udp_port [514 | <udp_port_number 6000-65535>] − Specifies the UDP port number that the syslog protocol is to use to send messages to the remote host.

ipaddress [<ipaddr> | <ipv6addr>] − Specifies the IPv4 or IPv6 address of the remote host to which syslog messages are to be sent.

state [enable | disable] − Allows the sending of syslog messages to

	the remote host, specified above, to be enabled and disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure a syslog host:

```
DGS-1210-28MP:5#  config syslog host 1 severity debug
Command: config syslog host 1 severity debug

Success.
DGS-1210-28MP:5#
```

delete syslog host

Purpose	To remove a previously configured syslog host from the Switch.
Syntax	**delete syslog host [<index 1-4> | all]**
Description	The **delete syslog host** command removes a previously configured syslog host from the Switch.
Parameters	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4. *all* − Specifies that the command applies to all hosts.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DGS-1210-28MP:5# delete syslog host all
Command: delete syslog host all

Success.
DGS-1210-28MP:5#
```

show syslog host

Purpose	To display the syslog hosts currently configured on the Switch.
Syntax	**show syslog host {<index 1-4>}**
Description	The **show syslog host** command displays the syslog hosts that are currently configured on the Switch.
Parameters	*<index 1-4>* − The syslog host index id. There are four available indices, numbered 1 to 4.
Restrictions	None.

Example usage:

To show Syslog host information:

```
DGS-1210-28MP:5# show syslog host
Command: show syslog host

Host 1
  IP Address: 1.1.2.1
  Severity  : Information
```

```
Facility : local0
UDP Port : 514
Status   : Enabled

Total Entries      : 1

DGS-1210-28MP:5#
```

cable diagnostic port

Purpose	To determine if there are any errors on the copper cables and the position where the errors may have occurred.
Syntax	**cable diagnostic port [<portlist > | all]**
Description	The **cable diagnostic port** command is used to determine if there are any errors on the copper cables and the position where the errors may have occurred. Cable length is detected as following range: <50m, 50~80, 80~100, >100m. Deviation is +/-5 meters, therefore "No Cable" may be displayed under "Test Result," when the cable used is less than 5 m in length. The Fault Distance will show “No Cable”, whether the fiber is connected to the port or not.
Parameters	*<portlist >* – A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To determine the copper cables and position of port 3 on the Switch:

```
DGS-1210-28MP:5# cable diagnostic port 3
Command: cable diagnostic port 3

 Perform Cable Diagnostics ...

 Port  Type   Link Status  Test Result   Fault Distance (meters)  Length(M)
 ----  -----  ----------- ------------- ------------------------- ---------
 3     GE     Link Down   Pair1:N/A     Pair1:No Cable            N/A
                          Pair2:OPEN    Pair2:1
                          Pair3:N/A     Pair3:N/A
                          Pair4:N/A     Pair4:N/A

DGS-1210-28MP:5#
```

show cpu port

Purpose	To display the statistics for packets forward to system CPU. The statistics is collected is type of packets.
Syntax	**show cpu port**
Description	The **show cpu port** command is used to To display the statistics for packets forward to system CPU. The statistics is collected is type of packets.

Parameters	None.
Restrictions	None.

Example usage:

To display the packet statictics of packet forward to CPU:

```
DGS-1210-28MP:5# show cpu port
Command: show cpu port

Type              Total     Diff
----------------- --------- ----------
ARP               1         +1
DHCP              0
DHCPv6            0
GVRP              0
ICMP              6         +6
ICMPv6            0
IGMP              0
LACP              0
LLDP              0
PPPoE             0
Reserved Multicast  0
STP               0
TELNET            0
UDP               0
```

reset cpu port

Purpose	To reset the statistics result for packets forward to system CPU.
Syntax	**reset cpu port**
Description	The **reset cpu port** command is used to to clear the current statistics of CPU port.
Parameters	None.
Restrictions	None.

Example usage:

To reset the packet statictics of packet forward to CPU:

```
DGS-1210-28MP:5# reset cpu port
Command: reset cpu port

Success.
```

13

FORWARDING DATABASE COMMANDS

The Forwarding Database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create fdb vlan	<vlan_name 20> <macaddr> port <port >
create multicast_fdb	<vlanid 1-4094><macaddr>
config multicast_fdb	< vlanid 1-4094> <macaddr> [add | delete] <portlist >
config fdb aging_time	<sec 10-600>
delete fdb	<vlan_name 20> <macaddr>
show multicast_fdb	{vlan <vlan_name 20> | mac_address <macaddr>}
show fdb	{port <portlist > | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
config multicast port_filtering_mode	[all | <portlist >] [forward_unregistered_groups | filter_unregistered_groups]
show multicast port_filtering_mode	

Each command is listed in detail, as follows:

create fdb vlan	
Purpose	To create a static entry in the unicast MAC address forwarding table (database)
Syntax	**create fdb vlan <vlan_name 20> <macaddr> port <port >**
Description	The **create fdb** command creates a static entry in the Switch's unicast MAC address forwarding database.
Parameters	*<vlan_name 20>* − The VLAN group that static MAC address would be bound. *<macaddr>* − The MAC address to be added to the forwarding table. *port <port >* − The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry:

```
DGS-1210-28MP:5# create fdb vlan test 00:12:34:56:78:90 port 2
Command: create fdb vlan test 00:12:34:56:78:90 port 2


Success.
```

create multicast_fdb	
Purpose	To create a static entry in the multicast MAC address forwarding table (database).
Syntax	**create multicast_fdb <vlanid 1-4094><macaddr>**
Description	The **create multicast_fdb** command creates a static entry in the multicast MAC address forwarding table (database).
Parameters	<*vlanid 1-4094*> − The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. <*macaddr*> − The MAC address to be added to the forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding:

```
DGS-1210-28MP:5# create multicast_fdb 1 01:00:5e:23:45:67
Command: create multicast_fdb 1 01:00:5E:23:45:67


Success.
```

config multicast_fdb	
Purpose	To configure the Switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <vlanid 1-4094> <macaddr> [add | delete] <portlist >**
Description	The **config multicast_fdb** command configures the multicast MAC address forwarding table.
Parameters	<*vlanid 1-4094*> − The item of the VLAN on which the MAC address resides. The range is between 1 and 4094. <*macaddr*> − The MAC address to be configured to the forwarding table. *add* − Specifies that the MAC address is to be added to the forwarding table. Delete will remove the MAC address from the forwarding table. *delete* − Specifies that the MAC address is to be removed from the forwarding table. <*portlist* > − A port or range of ports to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast MAC forwarding:

```
DGS-1210-28MP:5# config multicast_fdb 1 01:00:5e:23:45:67 add 3
Command: config multicast_fdb 1 01:00:5E:23:45:67 add 3


Success.
DGS-1210-28MP:5#
```

config fdb aging_time

Purpose	To set the aging time of the forwarding database.
Syntax	**config fdb aging_time <sec 10-600>**
Description	The **config fdb aging_time** command sets the aging time of the forwarding database. The aging time affects the learning process of the Switch. Dynamic forwarding table entries, which are made up of the source MAC addresses and their associated port numbers, are deleted from the table if they are not accessed within the aging time. The aging time can be from 0 to 630 minutes with a default value of 5 minutes. A very long aging time can result in dynamic forwarding table entries that are out-of-date or no longer exist. This may cause incorrect packet forwarding decisions by the Switch. If the aging time is too short however, many entries may be aged out too soon. This will result in a high percentage of received packets whose source addresses cannot be found in the forwarding table, in which case the Switch will broadcast the packet to all ports, negating many of the benefits of having a Switch.
Parameters	*<sec 10-600>* − The aging time for the MAC address forwarding database value, in seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To set the fdb aging time:

```
DGS-1210-28MP:5# config fdb aging_time 300
Command: config fdb aging_time 300

Success.
DGS-1210-28MP:5#
```

delete fdb

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	**delete fdb <vlan_name 20> <macaddr>**
Description	The **delete fdb** command deletes an entry in the Switch's MAC address forwarding database.
Parameters	*<vlan_name 20>* − The name of the VLAN on which the MAC address resides. *<macaddr>* − The MAC address to be removed from the forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DGS-1210-28MP:5# delete fdb test 00-12-34-56-78-90
Command: delete fdb test 00:12:34:56:78:90

Success.
DGS-1210-28MP:5#
```

show multicast_fdb	
Purpose	To display the contents of the Switch's multicast forwarding database.
Syntax	**show multicast_fdb {vlan <vlan_name 20> | mac_address <macaddr>}**
Description	The **show multicast_fdb** command displays the current contents of the Switch's multicast MAC address forwarding database.
Parameters	*vlan* <*vlan_name 20*> − The name of the VLAN on which the MAC address resides. *mac_address* <*macaddr*> − The MAC address that will be added to the forwarding table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-1210-28MP:5# show multicast_fdb
Command: show multicast_fdb


VLAN Name      : default
MAC Address    : 01-00-5E-23-45-67
Egress Ports   : 3
Mode           : Static

Total Entries      : 1

DGS-1210-28MP:5#
```

show fdb	
Purpose	To display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port > | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}**
Description	The **show fdb** command displays the current contents of the Switch's forwarding database.
Parameters	<*port* > − The port number corresponding to the MAC destination address. The Switch always forwards traffic to the specified device through this port. <*vlan_name 32*> − The name of the VLAN on which the MAC address resides. <*macaddr*> − The MAC address entry in the forwarding table. *static* − Specifies that static MAC address entries are to be displayed. *aging_time* − Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-1210-28MP:5# show fdb port 3
Command: show fdb port 3


VID  VLAN Name             MAC Address       Port  Type
---- ---------------------- ----------------- ----  ---------------
1    default                00-00-01-01-02-03 3     Permanent

Total Entries  : 1
DGS-1210-28MP:5#
```

To display the aging time:

```
DGS-1210-28MP:5# show fdb aging_time
Command: show fdb aging_time

Unicast MAC Address Aging Time = 300 sec

DGS-1210-28MP:5#
```

config multicast filter

Purpose	To configure multicast filtering.
Syntax	**config multicast filter <portlist> [filter | forward]**
Description	The **config multicast filter** command enables filtering of multicast addresses. When multicast filter enabled, only register multicast traffic can be forwarded.
Parameters	*<portlist]* - A port or range of ports to be configured. *filter* – filter unregister group *forward* – forward all multicast traffic
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast filtering

```
DGS-1210-28MP:5# config multicast filter 1-10 filter
Command: config multicast filter 1-10 filter


Success.
```

show multicast filter port_mode

Purpose	To display multicast filtering settings on the Switch.
Syntax	**show multicast filter port_mode**
Description	The **show multicast filter port_mode** command displays the multicast filtering settings.
Parameters	None.

Restrictions	None.

Example usage:

To show multicast filtering settings:

```
DGS-1210-28MP:5# show multicast filter port_mode
Command: show multicast filter port_mode

Multicast Filter Mode For Unregistered Group:
      Forwarding List: 11-28
      Filtering  List: 1-10

DGS-1210-28MP:5#
```

enable flood_fdb

Purpose	To enable the Switch's forwarding database on the Switch.
Syntax	**enable flood_fdb**
Description	The **enable flood_fdb** command enables dynamically learned entries from the Switch's forwarding database. Once flood_fdb enabled, MAC entries are learned/forwarded via system CPU which may cause utilization raised up.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable FDB dynamic entries:

```
DGS-1210-28MP:5# enable flood_fdb
Command: enable flood_fdb


Success.
DGS-1210-28MP:5#
```

disable flood_fdb

Purpose	To disable the Switch's forwarding database on the Switch.
Syntax	**disable flood_fdb**
Description	The **disable flood_fdb** command disables dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable FDB dynamic entries:

```
DGS-1210-28MP:5# disable flood_fdb
Command: disable flood_fdb
```

```
Success.
DGS-1210-28MP:5#
```

config flood_fdb

Purpose	To configure the Switch's forwarding database on the Switch.
Syntax	**config flood_fdb [log | trap] [enable | disable]**
Description	The **config flood_fdb** command configure notification (syslog and SNMP trap) when conflict condition detected by system.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure FDB dynamic entries:

```
DGS-1210-28MP:5# config flood_fdb trap disable log enable
Command: config flood_fdb trap disable log enable


Success.
DGS-1210-28MP:5#
```

show flood_fdb

Purpose	To display the Switch's forwarding database on the Switch.
Syntax	**show flood_fdb**
Description	The **show flood_fdb** command displays dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	None.

Example usage:

To display FDB dynamic entries:

```
DGS-1210-28MP:5# show flood_fdb
Command: show flood_fdb

Flooding FDB State : Enabled
Log State          : Disabled
Trap State         : Disabled

Value  VLAN ID    MAC Address       Time stamp
-------- ---------- ----------------- -----------------
DGS-1210-28MP:5#
```

clear flood_fdb

Purpose	To clear the MAC entry record for MAC conflict when flood_fdb enabled.

Syntax	**clear flood_fdb**
Description	The **clear flood_fdb** command clears dynamically learned entries from the Switch's forwarding database.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries:

```
DGS-1210-28MP:5# clear flood_fdb
Command: clear flood_fdb

Success.
DGS-1210-28MP:5#
```

create auto_fdb

Purpose	Used to discover (VLAN, MAC address and Port) for specified IP address and automatically created onto FDB.
Syntax	**create auto_fdb <ipaddr>**
Description	The **create auto_fdb** command is used to discover (VLAN, MAC address and Port) for specified IP address and automatically created onto FDB.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create auto_fdb entry:

```
DGS-1210-28MP:5# create auto_fdb 10.90.90.1
Command: create auto_fdb 10.90.90.1


Success.

DGS-1210-28MP:5#
```

show auto_fdb

Purpose	Used to display the information of particular IP address created in auto_fdb list.
Syntax	**show auto_fdb <ipaddr>**
Description	The **show auto_fdb** command is used to display information of IP address created in auto_fdb list..
Parameters	None.
Restrictions	None.

Example usage:

To display auto_fdb entries:

```
DGS-1210-28MP:5# show auto_fdb
```

```
Command: show auto_fdb

IP Address      VLAN ID   MAC Address         Port      Time Stamp
---------------  ----------  ------------------  ----------  ----------
10.90.90.1

DGS-1210-28MP:5#
```

delete auto_fdb

Purpose	Used to delete the auto_fdb entry.
Syntax	**delete auto_fdb <ipaddr>**
Description	The **delete auto_fdb** command is used to delete auto_fdb entry.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete auto_fdb entry:

```
DGS-1210-28MP:5# delete auto_fdb 10.90.90.1
Command: delete auto_fdb 10.90.90.1


Success.
```

14

BROADCAST STORM CONTROL COMMANDS

The Broadcast Storm Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config traffic control	[<portlist> | all] [broadcast {enable | disable} | multicast {enable | disable} | unicast {enable | disable}] action [drop | shutdown | dropbypps] threshold <value 0- 1024000> time_interval <time_interval 5-30> countdown {0 | <minutes (5-30)> | disable}
config traffic control auto_recover_time	[0 | <min 1-65535>]
show traffic control	{<portlist>}

Each command is listed in detail, as follows:

config traffic control

Purpose	To configure broadcast / multicast / unknown unicast traffic control.
Syntax	**config traffic control [<portlist> | all] [broadcast {enable | disable} | multicast {enable | disable} | unicast {enable | disable}] action [drop | shutdown | dropbypps] threshold <value 0- 1024000> time_interval <time_interval 5-30> countdown {0 | <minutes (5-30)> | disable}**
Description	The **config traffic control** command configures broadcast, multicast and unknown unicast storm control.
Parameters	*<portlist>* - A port or range of ports to be configured. *all* − Specifies all ports on the Switch are to be configured. *action* − Specifies the traffic control action to be drop or shutdown. 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. *drop* – Drop the packet when ingress rate over the threshold configured. When “drop” seleted, the measurement unit of threshold is kbit/second. *shutdown – Shutdown the specified ports* when ingress rate over the threshold configured. When “drop” seleted, the measurement unit of threshold is kbit/second. dropbypps - Drop the packet when ingress rate over the threshold configured. When “drop” seleted, the measurement unit of threshold is packet/second. *countdown [0 | <minutes 5-30>]* − Specifies the countdown time of traffic control. Value “0” represents countdown mechanism turned off. In other words, the configured action would be executed immediately once event occurred. *broadcast* –- Specify the broadcast storm status. *enable* - Enable broadcast storm control.

	disable - Disable broadcast storm control *multicast* –Specify the multicast storm status. *enable* - Enable multicast storm control. *disable* - Disable multicast storm control *unicast* –Specify the unicast packet storm status. *enable* - Enable unicast packet storm control. *disable* - Disable unicast packet storm control. *threshold <value 0-1024000>* − The upper threshold at which the specified traffic control is switched on. The value is the number of broadcast/multicast/dlf packets, in Kbps, received by the Switch that will trigger the storm traffic control measures. The value ranges in size from 0 to 1024000 Kbps. The default setting is 64 Kbit/sec. When action “drop” seleted, the measurement unit of threshold is packet/second. *<time_interval 5-30>* − Specifies the time interval of traffic control. Measurement unit is “minute”.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure traffic control and enable broadcast storm control system wide:

```
DGS-1210-28MP:5# config traffic control all multicast enable unicast disable
broadcast enable threshold 64
Command: config traffic control all multicast enable unicast disable broadcast
enable threshold 64

*Note: Setting count down for drop mode port was ignored.
Success.

DGS-1210-28MP:5#
```

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.
Syntax	**config traffic control auto_recover_time [0 | <min 1-65535>]**
Description	The **config traffic control auto_recover_time** command configures the auto recover time for traffic control.
Parameters	*[0 | <min 1-65535>]* – Specifies the auto recover time for traffic control The value is or from 1 to 65535.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure auto recover time for traffic control:

```
DGS-1210-28MP:5# config traffic control auto_recover_time 1000
Command: config traffic control auto_recover_time 1000

Success.

DGS-1210-28MP:5#
```

show traffic control

Purpose	To display current traffic control settings.
Syntax	**show traffic control {<portlist>}**
Description	The **show traffic control** command displays the current storm traffic control configuration on the Switch.
Parameters	*<portlist>* - A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display traffic control setting for ports 1-3:

```
DGS-1210-28MP:5# show traffic control 1-3
Command: show traffic control 1-3

Traffic Storm Control Trap : [None]

Port Thres  Broadcast Multicast Unicast   Action   Count    Time
     hold   Storm     Storm     Storm               down     Interval
---- ------- --------- --------- --------- -------- -------- --------
1    64      Enabled   Enabled   Disabled  Drop     0        0
2    64      Enabled   Enabled   Disabled  Drop     0        0
3    64      Enabled   Enabled   Disabled  Drop     0        0


Total Entries : 3

DGS-1210-28MP:5#
```

config traffic trap

Purpose	To configure the traffic control trap on the Switch.
Syntax	**config traffic trap [storm_cleared | storm_occured | both | none]**
Description	The **config traffic trap** command configures the current storm traffic trap configuration on the Switch.
Parameters	*storm_cleared* – A notification will be generated when a storm event is cleared. *storm_occured* – A notification will be generated when a storm event is detected. *both* – A notification will be generated both when a storm event is detected and cleared. *none* – No notification will be generated when storm event is detected or cleared.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure traffic trap setting:

```
DGS-1210-28MP:5# config traffic trap storm_cleared
```

```
Command: config traffic trap storm_cleared

Success.

DGS-1210-28MP:5#
```

15

QOS COMMANDS

The QoS commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config bandwidth_control	[<portlist > | all] {rx_rate [no_limit | <value 16-1000000>] | tx_rate [no_limit | <value 16-1000000>]}
show bandwidth_control	{[<portlist > | all]}
config qos mode	[802.1p | dscp | portbased]
show qos mode	
config scheduling_mechanism	[strict | wrr]
show scheduling_mechanism	
config dscp_mapping	dscp_value <value_list 0-63> queue <value 0-7>
show dscp_mapping	{dscp_value <value_list 0-63>}
config port_priority	[<portlist> | all] priority <value 0-7>
show port_priority	
show 802.1p user_priority	
show scheduling	

Each command is listed in detail, as follows:

config bandwidth_control	
Purpose	To configure bandwidth control on the Switch.
Syntax	**config bandwidth control [<portlist > | all] {rx_rate [no_limit | <value 16-1000000>] | tx_rate [no_limit | <value 16-1000000>]}**
Description	The **config bandwidth_control** command defines bandwidth control.
Parameters	*<portlist* > - A port or range of ports to be configured. *all* - Specifies that the **config bandwidth_control** command applies to all ports on the Switch. *rx_rate* - Enables ingress rate limiting • *no_limit* – Indicates no limit is defined. • *<value 16–1000000>*] – Indicates a range between 16-1000000 kbps. *tx_rate* – Enables egress rate limiting. • *no_limit* – Indicates no limit is defined. • *<value 16–1000000>]* – Indicates a range between 16-

	1000000 kbps.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure bandwidth control configuration:

```
DGS-1210-28MP:5# config bandwidth_control all tx_rate 10000
Command: config bandwidth_control all tx_rate 10000


Success.
```

show bandwidth_control

Purpose	To display bandwidth control settings on the Switch.
Syntax	**show bandwidth control {[<portlist > | all]}**
Description	The **show bandwidth_control** command displays bandwidth control.
Parameters	*<portlist >* – A port or range of ports to be configured. *all* – Specifies that the **show bandwidth_control** command applies to all ports on the Switch.
Restrictions	None.

Example usage:

T o display the bandwidth control configuration:

```
DGS-1210-28MP:5# show bandwidth_control
Command: show bandwidth_control


Port  Rx Rate    Tx Rate    Effective Rx  Effective Tx
     (Kbit/sec) (Kbit/sec) (Kbit/sec)    (Kbit/sec)
----  ---------- ---------- ------------  -------------
1    no limit   10000      no limit      no limit
2    no limit   10000      no limit      no limit
3    no limit   10000      no limit      no limit
4    no limit   10000      no limit      no limit
5    no limit   10000      no limit      no limit
6    no limit   10000      no limit      no limit
7    no limit   10000      no limit      no limit
8    no limit   10000      no limit      no limit
9    no limit   10000      no limit      no limit
10   no limit   10000      no limit      no limit
11   no limit   10000      no limit      no limit
12   no limit   10000      no limit      no limit
13   no limit   10000      no limit      no limit
14   no limit   10000      no limit      no limit
15   no limit   10000      no limit      no limit
16   no limit   10000      no limit      no limit
17   no limit   10000      no limit      no limit
```

config qos mode

Purpose	To configure the QoS mode.
Syntax	**config qos mode [802.1p | dscp | portbased]**
Description	The **config qos mode** command is used to configure the QoS mode on the Switch.
Parameters	*[802.1p* | *dscp* | *portbased]* – Specifies the QoS mode to be 802.1p, dscp or portbased.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the QoS mode to be portbased on the Switch:

```
DGS-1210-28MP:5#  config qos mode portbased
Command: config qos mode portbased

Success.
DGS-1210-28MP:5#
```

show qos mode

Purpose	To display the QoS mode.
Syntax	**show qos mode**
Description	The **show qos mode** command is used to display the QoS mode on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the QoS mode on the Switch:

```
DGS-1210-28MP:5#  show qos mode
Command: show qos mode

Qos mode  :  portbased
DGS-1210-28MP:5#
```

config scheduling_mechanism

Purpose	To configure the scheduling mechanism for the QoS function.
Syntax	**config scheduling_mechanism [strict | wrr]**
Description	The **config scheduling_mechanism** command configures the scheduling mechanism for the QoS function. It allows the user to select between a round robin (WRR) and a strict mechanism for emptying the priority classes of service of the QoS function. The Switch contains four hardware priority classes of service. Incoming packets must be mapped to one of these four hardware priority classes of service, or queues. This command is used to specify the rotation by which these four hardware priority queues are emptied. The Switch's default is to empty the four hardware priority queues in

	order − from the highest priority hardware queue (class 3) to the lowest priority hardware queue (class 0). Each queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. A lower priority hardware queue will be pre-empted from emptying its queue if a packet is received on a higher priority hardware queue. The packet received on the higher priority hardware queue transmits its packet before allowing the lower priority hardware queue to resume clearing its queue.
Parameters	*strict* – Specifies that the highest class of service is the first to be processed. That is, the highest class of service should finish emptying before the others begin. *wrr* – Specifies that the priority classes of service are to empty packets in a weighted roundrobin (WRR) order.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-1210-28MP:5# config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success.
DGS-1210-28MP:5#
```

show scheduling_mechanism

Purpose	To display the current traffic scheduling mechanisms in use on the Switch.
Syntax	**show scheduling_mechanism**
Description	The **show scheduling_mechanism** command displays the current traffic scheduling mechanisms in use on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the scheduling mechanism:

```
DGS-1210-28MP:5#  show scheduling_mechanism
Command: show scheduling_mechanism

Queue Mechanism       : strict
DGS-1210-28MP:5#
```

config dscp_mapping

Purpose	To configure the classes (queue) that each DSCP value maps to.
Syntax	**config dscp_mapping dscp_value <value_list 0-63> class <value 0-7>**
Description	The **config dscp_mapping** command enables mapping the DSCP value (the priority) to a specific queue (the class_id).
Parameters	<*value_list 0-63*> –The selected value of priority. The value may be

	between 0 and 63. *class <value 0-7>* – Specifies the priority to be mapped.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the DSCP value to particular class:

```
DGS-1210-28MP:5#  config dscp_mapping dscp_value 10 class 6
Command: config dscp_mapping dscp_value 10 queue 0

Success.
DGS-1210-28MP:5#
```

show dscp_mapping

Purpose	To display the setting of DSCP mapping.
Syntax	**show dscp_mapping {dscp_value <value_list 0-63>}**
Description	The **show dscp_mapping** command displays the mapping of DSCP value.
Parameters	*dscp_value <value_list 0-63>* - The selected value of priority will be dispalyed. The value may be between 0 and 63.
Restrictions	None.

Example usage:

To display the DSCP values:

```
DGS-1210-28MP:5# show dscp_mapping
Command: show dscp_mapping

DSCP  Priority
----  --------
0     0
1     0
2     0
3     0
4     0
5     0
6     0
7     0
8     0
9     0
10    6
```

config port_priority

Purpose	To configure the priority in port basis.
Syntax	**config port_priority [<portlist> | all] priority <value 0-7>**
Description	The **config port_priority** command used to define the priority for each physical port.

Parameters	*[<portlist> | all]* – A port or a range of port to be specified. *priority <value 0-7>* – Specifies the priority.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the priority class for port 1:

```
DGS-1210-28MP:5# config port_priority 1 priority 7
Command: config port_priority 1 priority 7


Success.
```

show port_priority

Purpose	To display the current configure priority value for each port.
Syntax	**show port_priority**
Description	The **config port_priority** command used to define the priority for each physical port.
Parameters	None.
Restrictions	None.

Example usage:

To display port priority value:

```
DGS-1210-28MP:5# show port_priority
Command: show port_priority


Port  Priority  Effective Priority
----  --------  ------------------
1     7         7
2     0         0
3     0         0
4     0         0
5     0         0
6     0         0
```

show 802.1p user_priority

Purpose	To display the table that 802.1p values maps to class queue.
Syntax	**show 802.1p user_priority**
Description	The **show 802.1p user_priority** command used to display the table that 802.1p values maps to class queue.
Parameters	None.
Restrictions	None.

Example usage:

To display 802.1 priority values:

```
DGS-1210-28MP:5# show 802.1p user_priority
Command: show 802.1p user_priority


802.1p Priority   Queue
---------------   ------
0                  2
1                  0
2                  1
3                  3
4                  4
5                  5
6                  6
7                  7

DGS-1210-28MP:5#
```

show scheduling

Purpose	To display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling**
Description	The **show scheduling** command displays the current configuration for the maximum number of packets (*max_packet*) value assigned to the four priority classes of service on the Switch. The Switch empties the four hardware queues in order, from the highest priority (class 3) to the lowest priority (class 0).
Parameters	None.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DGS-1210-28MP:5# show scheduling
Command: show scheduling


Queue  Weight
-----  ------
0       1
1       2
2       3
3       4
4       5
5       6
6       7
7       8

DGS-1210-28MP:5#
```

16

RMON COMMANDS

The RMON commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable rmon	
disable rmon	
create rmon alarm	<alarm_index 1-65535> <OID_variable 255> <interval 1-2147482647> [absolute | delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> {[owner <owner_string 32>]}
delete rmon alarm	<alarm_index 1-65535>
create rmon collection stats	<stats_index 1-65535> port <ifindex> owner <owner_string 32>
delete rmon collection stats	<stats_index 1-65535>
create rmon collection history	<hist_index 1-65535> port <ifindex> {buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 32>}
delete rmon collection history	<hist_index 1-65535>
create rmon event	<event_index 1-65535> description <desc_string 128> {[log | owner <owner_string 32> | trap <community_string 32>]}
delete rmon event	<event_index 1-65535>
show rmon	{statistics <stats_index 1-65535> | alarms | events | history <hist_index 1-65535> | overview}

Each command is listed in detail, as follows:

enable rmon	
Purpose	To enable remote monitoring (RMON) status for the SNMP function.
Syntax	**enable rmon**
Description	The **enable rmon** command enables remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the RMON feature on the Switch:

```
DGS-1210-28MP:5# enable rmon
Command: enable rmon
```

```
Success.
DGS-1210-28MP:5#
```

disable rmon

Purpose	To disable remote monitoring (RMON) status for the SNMP function.
Syntax	**disable rmon**
Description	The **disable rmon** command disables remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the RMON feature on the Switch:

```
DGS-1210-28MP:5# disable rmon
Command: disable rmon

Success.
DGS-1210-28MP:5#
```

create rmon alarm

Purpose	To allow the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.
Syntax	**create rmon alarm <alarm_index 1-65535> <OID_variable 255> <interval 1-2147482647> [absolute | delta] rising-threshold <value 0-2147483647> <rising_event_index 1-65535> falling-threshold <value 0-2147483647> <falling_event_index 1-65535> {[owner <owner_string 32>]}**
Description	The **create rmon alarm** command allows the user to configure the network alarms. Network alarms occur when a network problem, or event, is detected.
Parameters	*<alarm_index>* − Specifies the alarm number. *<OID_variable 255>* − Specifies the MIB variable value. *<interval 1-2147482647>* − Specifies the alarm interval time in seconds. *[absolute | delta]* − Specifies the sampling method for the selected variable and comparing the value against the thresholds. The possible values are absolute and delta: • *absolute* –Compares the values directly with the thresholds at the end of the sampling interval. • *delta* –Subtracts the last sampled value from the current value. The difference in the values is compared to the threshold. *rising-threshold <value 0-2147483647>* − Specifies the rising counter value that triggers the rising threshold alarm. *<rising_event_index 1-65535>* − Specifies the event that triggers the specific alarm.

	falling-threshold <*value 0-2147483647*> − Specifies the falling counter value that triggers the falling threshold alarm. *<falling_event_index 1-65535>* − Specifies the event that triggers the specific alarm. The possible field values are user defined RMON events. *owner* <*owner_string 32*> − Specifies the device or user that defined the alarm.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON alarm on the Switch:

```
DGS-1210-28MP:5# create rmon alarm 20 1 absolute rising-threshold
200 2falling-threshold 100 1 owner dlink
Command: create rmon alarm 20 1 absolute rising-threshold 200
2falling-threshold 100 1 owner dlink


Success.
DGS-1210-28MP:5#
```

delete rmon alarm

Purpose	To remove the network alarms.
Syntax	**delete rmon alarm <alarm_index 1-65535>**
Description	The **delete rmon alarm** command removes the network alarms.
Parameters	*<alarm_index 1-65535>* − Specifies the alarm number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON alarm on the Switch:

```
DGS-1210-28MP:5# delete rmon alarm 100
Command: delete rmon alarm 100

Success.
DGS-1210-28MP:5#
```

create rmon collection stats

Purpose	To allow user to configure the rmon stats settings on the Switch.
Syntax	**create rmon collection stats <stats_index 1-65535> port <ifindex> owner <owner_string 32>**
Description	The **create rmon collection stats** command allows user to configure the rmon stats settings on the Switch.
Parameters	*<stats_index 1-65535>* − Specifies the stats number. *port <ifindex>* − Specifies the port from which the RMON information was taken. *owner <owner_string 32>* − Specifies the device or user that defined

	the stats.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection stats on the Switch:

```
DGS-1210-28MP:5#  create rmon collection stats 100 port 1 owner dlink
Command: create rmon collection stats 100 port 1 owner dlink

Success.
DGS-1210-28MP:5#
```

delete rmon collection stats

Purpose	To remove the network collection stats.
Syntax	**delete rmon collection stats <stats_index 1-65535>**
Description	The **delete rmon collection stats** command removes the network collection stats on the Switch.
Parameters	*<stats_index 1-65535>* − Specifies the stats number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON collection stats on the Switch:

```
DGS-1210-28MP:5# delete rmon collection stats 2
Command: delete rmon collection stats 2

Success.
DGS-1210-28MP:5#
```

create rmon collection history

Purpose	To allow user to configure the rmon history settings on the Switch.
Syntax	**create rmon collection history <hist_index 1-65535> port <ifindex> {buckets <buckets_req 1-50> interval <interval 1-3600> owner <owner_string 32>}**
Description	The **create rmon collection history** command allows user to configure the rmon history settings on the Switch.
Parameters	*<hist_index 1-65535>* − Indicates the history control entry number. *port <ifindex>* − Specifies the port from which the RMON information was taken. *buckets <buckets_req 1-50>* − Specifies the number of buckets that the device saves. *interval <interval 1-3600>* − Specifies in seconds the time period that samplings are taken from the ports. The field range is *1-3600*. The default is *1800* seconds (equal to 30 minutes). *owner <owner_string 127>* − Specifies the RMON station or user that requested the RMON information.

Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection history on the Switch:

```
DGS-1210-28MP:5#  create rmon collection history 120 port 1 buckets 10
Command: create rmon collection history 120 port 1 buckets 10

Success.
DGS-1210-28MP:5#
```

delete rmon collection history

Purpose	To remove the network collection history.
Syntax	**delete rmon collection history <hist_index 1-65535>**
Description	The **delete rmon collection history** command removes the network collection history on the Switch.
Parameters	*<hist_index 1-65535>* − Specifies the alarm history number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON collection history on the Switch:

```
DGS-1210-28MP:5# delete rmon collection history 2
Command: delete rmon collection history 2

Success.
DGS-1210-28MP:5#
```

create rmon event

Purpose	To provide user to configure the settings of rmon event on the Switch.
Syntax	**create rmon event <event_index 1-65535> description <desc_string 128> {[log | owner <owner_string 32> | trap <community_string 32>]}**
Description	The **create rmon event** command allows user to provides user to configure the settings of rmon event on the Switch.
Parameters	*<event_index 1-65535>* − Specifies the event number. *description <desc_string 128>* − Specifies the user-defined event description. *log* − Indicates that the event is a log entry. *owner <owner_string 32>* − Specifies the time that the event occurred. *trap <community_string 32>* − Specifies the community to which the event belongs.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RMON collection history on the Switch:

```
DGS-1210-28MP:5# create rmon event 125 description linkrmon owner dlink
Command: create rmon event 125 description linkrmon owner dlink

Success.
DGS-1210-28MP:5#
```

delete rmon event

Purpose	To remove the network event.
Syntax	**delete rmon event <event_index 1-65535>**
Description	The **delete rmon event** command removes the network event on the Switch.
Parameters	*<event_index 1-65535>* − Specifies the event number to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a RMON event on the Switch:

```
DGS-1210-28MP:5# delete rmon event 2
Command: delete rmon event 2

Success.
DGS-1210-28MP:5#
```

show rmon

Purpose	To display remote monitoring (RMON) status for the SNMP function.
Syntax	**show rmon {statistics <stats_index 1-65535> | alarms | events | history <hist_index 1-65535> | overview}**
Description	The **show rmon** command displays remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	*statistics <stats_index 1-65535>* − Specify the index of RMON statistics to be displayed. *alarms* – Specify the RMON alarm to be displayed. *events* − Specify the RMON events to be displayed. *history <hist_index 1-65535>* − Specify the RMON history to be displayed. *overview* – Display the RMON overview.
Restrictions	None.

Example usage:

To display the RMON feature on the Switch:

```
DGS-1210-28MP:5#  show rmon statistics 100 alarms events
```

```
Command: show rmon statistics 100 alarms events

RMON is Enabled
Collection 100 on 1 is active, and owned by dlink,
 Monitors ifEntry.1.1 which has
 Received 0 octets, 0 packets,
 0 broadcast and 0 multicast packets,
 0 undersized and 0 oversized packets,
 0 fragments and 0 jabbers,
 0 CRC alignment errors and 0 collisions.
 # of packets received of length (in octets):
 64: 0, 65-127: 0, 128-255: 0,
 256-511: 0, 512-1023: 0, 1024-1518: 0
Alarm table is empty
Event table is empty


DGS-1210-28MP:5#
```

17

PORT MIRRORING COMMANDS

The Port Mirroring commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable mirror	
disable mirror	
create mirror	group_id <value 1-4>
delete mirror	group_id <value 1-4>
config mirror	group_id <value 1-4> [target_port <port> | [add | delete] source ports <portlist> [rx |x | both] | state [enable | disable]]
show mirror	group_id <value 1-4>

Each command is listed in detail, as follows:

enable mirror	
Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	**enable mirror**
Description	The **enable mirror** command, combined with the disable mirror command below, allows the user 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 or operator-level users can issue this command.

Example usage:

To enable the mirroring feature:

```
DGS-1210-28MP:5# enable mirror
Command: enable mirror

Success.
DGS-1210-28MP:5#
```

disable mirror	
Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	**disable mirror**
Description	The **disable mirror** command, combined with the enable mirror command above, allows the user 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 or operator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DGS-1210-28MP:5# disable mirror
Command: disable mirror

Success.
DGS-1210-28MP:5#
```

create mirror

Purpose	Used to create a port mirroring group.
Syntax	**create mirror group_id <value 1-4>**
Description	The **create mirror** command allows a port to have all of its traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, one can specify that only traffic received by or sent by one or both is mirrored to the target port.
Parameters	*group_id <value 1-4>* − Specifies the mirror ID to be created.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create the mirroring ID:

```
DGS-1210-28MP:5# create mirror group_id 1
Command: create mirror group_id 1

Success.
```

delete mirror

Purpose	Used to delete a port mirroring group.
Syntax	**delete mirror group_id <value 1-4>**
Description	The **delete mirror** command is used to delete specify mirror group
Parameters	*group_id <value 1-4>* − Specifies the mirror ID to be created.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create the mirroring ID:

```
DGS-1210-28MP:5# delete mirror group_id 1
Command: delete mirror group_id 1
```

Success.

config mirror

Purpose	To configure a mirror port − source port pair on the Switch.
Syntax	**config mirror group_id <value 1-4> [target_port <port> | [add | delete] source ports <portlist> [rx |x | both] | state [enable | disable]]**
Description	The **config mirror** command offer user flexibility to configure variable combination of target/source port; ingree/egree traffic.
Parameters	*group_id <int 1-4>* − Specifies the mirror ID. *target <port>* − Specifies the port that mirrors traffic forwarding. *[add | delete]* − Specifies to add or delete the target port. *source ports <portlist >* – Specifies the port or ports being mirrored. This cannot include the target port. *rx* – Allows mirroring of packets received by (flowing into) the source port. *tx* – Allows mirroring of packets sent to (flowing out of) the source port. *both* – Allows mirroring of all the packets received or sent by the source port. *state* – To turn off/on particular mirror group. *Comment*: The user can define up to 8 source ports and one destination port. One source port can be configured each time using one CLI command, So in order to configure multiple source ports, multiple CLI commands should be used.
Restrictions	A target port cannot be listed as a source port. Only Administrator or operator-level users can issue this command.

Example usage:

To configure mirror group:

DGS-1210-28MP:5# config mirror group_id 1 target_port 7
Command: config mirror group_id 1 target_port 7

Success.

DGS-1210-28MP:5# config mirror group_id 1 add source ports 9-16 both
Command: config mirror group_id 1 add source ports 9-16 both

Success.

show mirror

Purpose	To show the current port mirroring configuration on the Switch.
Syntax	**show mirror {id <int 1-4>}**

Description	The **show mirror** command displays the current port mirroring configuration on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display mirroring ID 1 configuration:

```
DGS-1210-28MP:5# show mirror group_id 1
Command: show mirror group_id 1

Port Mirror is Enabled

ID   Target Port  Ingress port   Egress port    Both         State
---  -----------  ------------   ------------   ------------ --------
1    7            9-16           9-16           9-16         Enabled
DGS-1210-28MP:5#
```

18

VLAN COMMANDS

The VLAN commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create vlan	<vlan_name 20> tag <vlanid 2-4094>
delete vlan	[<vlan_name 20> | vlanid <vidlist 2-4094>]
config vlan	[<vlan_name 20> | vlanid <int 1-4094>] [[add [tagged | untagged] | delete] <portlist >
show vlan	{<vlan_name 20> | vlanid <vidlist 1-4094> | ports <portlist >}
enable asymmetric_vlan	
disable asymmetric_vlan	
show asymmetric_vlan	
enable management vlan	
disable management vlan	
config management vlan	vlanid <vlanid 1-4094>
show management vlan	
show port_vlan pvid	
enable voice_vlan	{ vlanid <vlanid (1-4094)> | < vlan_name (32) > }
disable voice_vlan	
config voice_vlan aging_time	<integer (1-120)>
config voice_vlan priority	<integer (0-7)>
config voice_vlan oui	{ add <macaddr> description <string (20)> [mask <macmask>] | delete <macaddr> }
config voice_vlan ports	<portlist> auto dectection { enable { tag | untag } | disable }
config voice_vlan log state	{ enable | disable }
show voice_vlan	[{ oui | ports <portlist> | { { lldp_med voice_device | voice_device } { all | ports <portlist> } } }]
enable surveillance_vlan	{ vlanid <vlanid (1-4094)> | < vlan_name (32) > }

Command	Parameter
disable surveillance_vlan	
config surveillance_vlan aging_time	<integer (1-120)>
config surveillance_vlan priority	<integer (0-7)>
config surveillance_vlan log state	{ enable | disable }
config surveillance_vlan onvif_discover_port	{554 | <integer (1025-65535)>}
config surveillance_vlan oui	{add | delete} <macaddr> <macmask> [component_type {vms | vms_client | video_encoder | network_storage | other} description <desc (32)>]
config surveillance_vlan ports	{<portlist> | all} state {enable | disable}
config surveillance_vlan onvif_ipc	<ip_addr> [mac <macaddr>] [description <desc (32)> | state {enable | disable}]
config surveillance_vlan onvif_nvr	<ip_addr> [mac <macaddr>] description <desc (32)>
show surveillance_vlan onvif_ipc_ports	[<portlist>] {brief | detail}
show surveillance_vlan onvif_nvr_ports	[<portlist>] [ipc_list]
show surveillance_vlan	[{ oui | ports [<portlist>] | device [ports <portlist>] }]

Each command is listed in detail, as follows:

create vlan	
Purpose	To create a VLAN on the Switch.
Syntax	**create vlan <vlan_name 20> tag <vlanid 2-4094>**
Description	The **create vlan** command creates a VLAN on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN to be created. *tag <vlanid 2-4094>* − The VLAN ID of the VLAN to be created. The allowed values range from 2 to 4094.
Restrictions	Each VLAN name can be up to 32 characters. If the VLAN is not given a tag, it will be a port-based VLAN. Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 3:

```
DGS-1210-28MP:5# create vlan v1 tag 3
```

```
Command: create vlan v1 tag 3

Success.
DGS-1210-28MP:5#
```

delete vlan

Purpose	To delete a previously configured VLAN on the Switch.
Syntax	**delete vlan [<vlan_name 20> | vlanid <vidlist 2-4094>]**
Description	The **delete vlan** command deletes a previously configured VLAN on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN to be deleted. *vlanid <vidlist 2-4092>* − The VLAN of the VLAN to be deleted.
Restrictions	Only administrator or operator-level users can issue this command. A user is required to disable Guest VLAN before deleting a VLAN.

Example usage:

To remove a VLAN group:

```
DGS-1210-28MP:5# delete vlan vlanid 2
Command: delete vlan vlanid 2

Success.
DGS-1210-28MP:5#
```

config vlan

Purpose	To add additional ports to a previously configured VLAN and to modify a VLAN name.
Syntax	**config vlan [<vlan_name 20> | vlanid <int 1-4094>] [[add [tagged | untagged] | delete] <portlist >**
Description	The **config vlan** command allows the user to add or delete 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 untagged.
Parameters	*<vlan_name 20>* − The name of the VLAN to be configure. *vlanid <int 1-4094 >* − The ID of the VLAN to which to add ports. *add* − Specifies that ports are to be added to a previously created vlan. *delete* - Specifies that ports are to be deleted from a previously created vlan. *tagged* − Specifies the additional ports as tagged. *untagged* − Specifies the additional ports as untagged. *<portlist >* − A port or range of ports to be added to or deleted from the VLAN.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure a port into particular VLAN group:

```
DGS-1210-28MP:5#  config vlan vlanid 1 add tagged 1-
```

```
3
Command: config vlan vlanid 1 add tagged 1-3


Success.
DGS-1210-28MP:5#
```

show vlan

Purpose	To display the current VLAN configuration on the Switch
Syntax	**show vlan {<vlan_name 20> | vlanid <vidlist 1-4094> | ports <portlist >}**
Description	The **show vlan** command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.
Parameters	*<vlan_name 20>* − Specify the VLAN id to be displayed. *vlanid <vidlist 1-4094>* − Specify the VLAN id to be displayed. ports <portlist > − Specify the ports to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-1210-28MP:5#  show vlan
Command: show vlan

VID             : 1         VLAN NAME     : default
VLAN Type       : Static
Member Ports    :
Untagged Ports  : 4-10

VID             : 100       VLAN NAME     : rd1
VLAN Type       : Static
Member Ports    :
Untagged Ports  :

DGS-1210-28MP:5#
```

enable asymmetric_vlan

Purpose	To enable Asymmetric VLAN on the switch.
Syntax	**enable asymmetric_vlan**
Description	The **enable asymmetric_vlan** command, along with the **disable enable asymmetric_vlan** command below, is used to enable and disable Asymmetric VLAN on the Switch
Parameters	None.

Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Asymettric VLAN on the switch:

```
DGS-1210-28MP:5# enable asymmetric_vlan
Command: enable asymmetric_vlan

Success.
DGS-1210-28MP:5#
```

disable asymmetric_vlan

Purpose	To disable Asymmetric VLAN on the switch.
Syntax	**disable asymmetric_vlan**
Description	The **disable asymmetric_vlan** command, along with the **enable asymmetric_vlan** command below, is used to disable and enable Asymmetric VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable asymmetric_vlan on the switch:

```
DGS-1210-28MP:5# disable asymmetric_vlan
Command: disable asymmetric_vlan

Success.
DGS-1210-28MP:5#
```

show asymmetric_vlan

Purpose	To display the Asymmetric VLAN status on the Switch.
Syntax	**show asymmetric_vlan**
Description	The **show asymmetric_vlan** command displays the Asymmetric VLAN status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display Asymmetric VLAN status:

```
DGS-1210-28MP:5# show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN : Enable
DGS-1210-28MP:5#
```

enable management vlan

Purpose	To enable the management VLAN on the Switch.
Syntax	**enable management vlan**
Description	The **enable management vlan** command enables the management VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable management VLAN on the switch:

```
DGS-1210-28MP:5# enable management vlan
Command: enable management vlan

Success.
DGS-1210-28MP:5#
```

disable management vlan

Purpose	To disable the management VLAN on the Switch.
Syntax	**disable management vlan**
Description	The **disable management vlan** command disables the management VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable management VLAN on the switch:

```
DGS-1210-28MP:5# disable management vlan
Command: disable management vlan

Success.
DGS-1210-28MP:5#
```

config management vlan

Purpose	To configure the management VLAN on the Switch.
Syntax	**config management vlanid <vlanid 1-4094>**
Description	The **config management vlan** command configures the management VLAN on the Switch.
Parameters	*vlanid <vlanid 1-4094>* − Specifies the management VLAN ID on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the management VLAN on the switch:

```
DGS-1210-28MP:5# config management vlanid 33
```

```
Command: config management vlanid 33


Success.
```

show management vlan

Purpose	To display the management VLAN on the Switch.
Syntax	**show management vlan**
Description	The **show management vlan** command displays the management VLAN information on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the management VLAN on the switch:

```
DGS-1210-28MP:5# show management vlan
Command: show management vlan

management vlan is enable

management vlan id  : 33
management vlan name: VLAN33
DGS-1210-28MP:5#
```

show port_vlan pvid

Purpose	To display the port PVID of VLAN on the Switch.
Syntax	**show port_vlan pvid**
Description	The **show port_vlan pvid** command displays the port PVID of VLAN on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the port PVID of VLAN on the switch:

```
DGS-1210-28MP:5#  show port_vlan pvid
Command: show port_vlan pvid

Port     PVID
---------------------
1        1
2        1
3        1
4        1
5        1
6        1
```

```
7        1
8        1
9        1
10       1
DGS-1210-28MP:5#
```

enable voice_vlan

Purpose	To assign the particular VLAN as Voice VLAN.
Syntax	**enable voice_vlan [vlanid <vlanid (1-4094)> | < vlan_name (32) >]**
Description	Voice VLAN is a VLAN used to carry voice traffic from IP phone. The quality of service (QoS) for voice traffic shall be configured higner than normal traffic to ensure the quality of sound.
Parameters	*<vlanid (1-4094)>* - Specifies all VLANs or VLAN id to be displayed. *<vlan_name>* - Specifies the name of VLAN
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To assign the particular VLAN as Voice VLAN:

```
DGS-1210-28:5# create vlan vlanid 5
Command: create vlan vlanid 5

Success.
DGS-1210-28:5# enable voice_vlan vlanid 5
Command: enable voice_vlan vlanid 5

Success.
DGS-1210-28:5# show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
Voice VLAN           : 5
Priority             : 5
Aging Time           : 1 hours
Log State            : Disabled
Member Ports         :
Dynamic Member Ports :

DGS-1210-28:5#
```

disable voice_vlan

Purpose	To disable Voice VLAN function.
Syntax	**disable voice_vlan**
Description	To disable Voice VLAN function
Parameters	None

Restrictions	Only administrator or operator-level users can issue this command.

config voice_vlan aging_time

Purpose	To specify the aging time of dynamic Voice VLAN member port.
Syntax	**config voice_vlan aging_time <integer (1-120)>**
Description	To specify the aging time of dynamic Voice VLAN member port
Parameters	*<integer (1-120)>* - in range of 1-120 hours
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specify the aging time of dynamic Voice VLAN member port:

```
DGS-1210-28:5# config voice_vlan aging_time 2
Command: config voice_vlan aging_time 2

Success.
DGS-1210-28:5# show voice_vlan
Command: show voice_vlan

Voice VLAN State     : Enabled
Voice VLAN           : 5
Priority             : 5
Aging Time           : 2 hours
Log State            : Disabled
Member Ports         :
Dynamic Member Ports :

DGS-1210-28:5#
```

config voice_vlan priority

Purpose	To specify the 802.1p priority value used in voice traffic.
Syntax	**config voice_vlan priority <integer (0-7)>**
Description	To specify the 802.1p priority value used in voice traffic.
Parameters	*<integer (0-7)>* - in range of 0-7 of 802.1p priority value
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specify the 802.1p priority value used in voice traffic:

```
DGS-1210-28:5# config voice_vlan priority 7
Command: config voice_vlan priority 7



Success.

DGS-1210-28:5# show voice_vlan
```

```
Command: show voice_vlan

Voice VLAN State     : Enabled
Voice VLAN           : 5
Priority             : 7
Aging Time           : 2 hours
Log State            : Disabled
Member Ports         : 8
Dynamic Member Ports : 1

DGS-1210-28:5#
```

config voice_vlan oui

Purpose	To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature.
Syntax	**config voice_vlan oui [add <macaddr> description <string (20)> { mask <macmask> } | delete <macaddr>]**
Description	To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature. The OUI can be determined as range list by configuring MAC mask.
Parameters	*<macaddr>* - To specify the MAC address either by XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX format *<macmask>* - To specify the mask of MAC address indentified
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature:

```
DGS-1210-28:5# config voice_vlan oui add 00-12-34-00-00-00 description
DLINK_TEST
Command: config voice_vlan oui add 00-12-34-00-00-00 description DLINK_TEST

Success.
DGS-1210-28:5# config voice_vlan oui add 00:23:45:00:00:01 description
DLINK_MASK mask ff:ff:ff:ff:ff:ff
Command: config voice_vlan oui add 00:23:45:00:00:01 description DLINK_MASK
mask ff:ff:ff:ff:ff:ff

Success.
DGS-1210-28:5# show voice_vlan oui
Command: show voice_vlan oui

ID      Description      Telephony OUI       OUI Mask
--  ----------------  ----------------  ----------------
1   DLINK_TEST        00-12-34-00-00-00  FF-FF-FF-00-00-00
2   DLINK_MASK        00-23-45-00-00-01  FF-FF-FF-FF-FF-FF

Total Entries : 2
```

```
DGS-1210-28:5#
```

config voice_vlan ports

Purpose	To change the the state of auto detection feature in Voice VLAN.
Syntax	**config voice_vlan ports <portlist> auto dectection [enable { tag | untag } | disable]**
Description	To change the the state of auto detection feature in Voice VLAN.
Parameters	*<portlist>* − A port, range of ports which would configured for Voice VLAN auto detection state. *{ tag | untag }* – Determine the port rule once the MAC address (OUI) hits the value configured
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature:

```
DGS-1210-28:5# config voice_vlan ports 1 auto dectection enable untag
Command: config voice_vlan ports 1 auto dectection enable untag



Success.

DGS-1210-28:5# config voice_vlan ports 8 auto dectection enable tag
Command: config voice_vlan ports 8 auto dectection enable tag



Success.

DGS-1210-28:5# show voice_vlan voice_device all
Command: show voice_vlan voice_device all

Ports   Voice Device
-----   -----------------
1       00-12-34-00-00-01
8       00-23-45-00-00-01

DGS-1210-28:5# show vlan vlanid 5
Command: show vlan vlanid 5

VID             : 5       VLAN NAME     : VLAN5
VLAN Type       : Voice VLAN
VLAN Advertisement : Disabled
Member Ports    : 1,8
Tagged Ports    : 8
Untagged Ports  : 1
Forbidden Ports : 1
```

config voice_vlan log state

Purpose	To change the the state of logging the event of Voice VLAN.
Syntax	**config voice_vlan log state [enable | disable]**
Description	To change the the state of logging the event of Voice VLAN.
Parameters	*enable* – Enable the logging machanism *disable* – Disable the logging mechanism
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for Voice VLAN auto detection feature:

```
DGS-1210-28:5# config voice_vlan log state enable
Command: config voice_vlan log state enable



Success.

DGS-1210-28:5# show log
Command: show log

Index  Time                 Log Text
-----  -------------------- ----------------------------------------
 10    Mar  6 17:20:55:Voice Vlan-6: Port 8 add into voice VLAN 5
  9    Mar  6 17:20:55:Voice Vlan-6: New voice device detected (Port:8, MAC:0-23-45-
0-0-1)
  8    Mar  6 17:20:54:Voice Vlan-6: Port 1 add into voice VLAN 5
  7    Mar  6 17:20:54:Voice Vlan-6: New voice device detected (Port:1, MAC:0-12-34-
0-0-1)
  6    Mar  6 17:20:40:LinkStatus-6: Port 8 link up, 100Mbps FULL duplex
  5    Mar  6 17:20:38:Voice Vlan-6: Port 8 remove from voice VLAN 5
  4    Mar  6 17:20:38:LinkStatus-6: port 8 link down
  3    Mar  6 17:20:36:LinkStatus-6: Port 1 link up, 100Mbps FULL duplex
  2    Mar  6 17:20:33:Voice Vlan-6: Port 1 remove from voice VLAN 5
  1    Mar  6 17:20:33:LinkStatus-6: port 1 link down



DGS-1210-28:5#
```

show voice_vlan

Purpose	Used to show Voice VLAN global status, per port status, and dynamic learned device.
Syntax	**show voice_vlan [{ oui | ports <portlist> | { { lldp_med voice_device | voice_device } { all | ports <portlist> } } }]**
Description	To change the the state of logging the event of Voice VLAN.

Parameters	*oui* – Specify the Voice VLAN OUI parameters configured. *<portlist>* –A port, range of ports would be displaied *lldp_med voice_device* – Specify the dynamic device learned by LLDP-MED mechanism *voice_device* – Specify the dynamic devices learned by OUI.mechanism
Restrictions	None.

Example usage:

To show Voice VLAN global status, per port status, and dynamic learned device:

```
DGS-1210-28:5# show voice_vlan oui
Command: show voice_vlan oui

ID      Description       Telephony OUI       OUI Mask
--   -----------------   -----------------   -----------------
1    DLINK_TEST          00-12-34-00-00-00   FF-FF-FF-00-00-00
2    DLINK_MASK          00-23-45-00-00-01   FF-FF-FF-FF-FF-FF

Total Entries : 2
DGS-1210-28:5# show voice_vlan voice_device all
Command: show voice_vlan voice_device all


Ports   Voice Device
-----   -----------------
1       00-12-34-00-00-01
8       00-23-45-00-00-01

Total Entries : 2
```

enable surveillance_vlan

Purpose	To assign the particular VLAN as surveillance VLAN.
Syntax	**enable surveillance_vlan [vlanid <vlanid (1-4094)> | < vlan_name (32) >]**
Description	Surveillance VLAN is a VLAN used to carry video traffic of IP cameras. The quality of service (QoS) for voice traffic shall be configured higner than normal traffic to ensure the quality of video.
Parameters	*<vlanid (1-4094)>* - Specifies all VLANs or VLAN id to be displayed. *<vlan_name>* - Specifies the name of VLAN
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To assign the particular VLAN as surveillance VLAN:

```
DGS-1210-28:5# create vlan vlanid 5
Command: create vlan vlanid 5

Success.
DGS-1210-28MP:5# enable surveillance_vlan vlanid 5
```

```
Command: enable surveillance_vlan vlanid 5


Success
```

disable surveillance_vlan

Purpose	To disable surveillance vlan function.
Syntax	**disable surveillance_vlan**
Description	To **disa**ble surveillance vlan function
Parameters	None
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To assign the particular VLAN as surveillance VLAN:

```
DGS-1210-28MP:5# disable surveillance_vlan
Command: disable surveillance_vlan


Success.
```

config surveillance_vlan aging_time

Purpose	To specify the aging time of dynamic surveillance VLAN member port.
Syntax	**config surveillance_vlan aging_time <integer (1-120)>**
Description	To specify the aging time of dynamic surveillance VLAN member port
Parameters	*<integer (1-120)>* - in range of 1-120 hours
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specify the aging time of dynamic surveillance VLAN member port:

```
DGS-1210-28MP:5# config surveillance_vlan aging_time 30
Command: config surveillance_vlan aging_time 30


Success.
```

config surveillance_vlan priority

Purpose	To specify the 802.1p priority value used in surveillance traffic.
Syntax	**config surveillance_vlan priority <integer (0-7)>**
Description	To specify the 802.1p priority value used in surveillance traffic.
Parameters	*<integer (0-7)>* - in range of 0-7 of 802.1p priority value
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specify the 802.1p priority value used in surveillance traffic:

```
DGS-1210-28MP:5# config surveillance_vlan priority 6
Command: config surveillance_vlan priority 6

Success.

DGS-1210-28MP:5#
```

config surveillance_vlan log state

Purpose	To change the the state of logging the event of surveillance VLAN.
Syntax	**config surveillance_vlan log state [enable | disable]**
Description	To change the the state of logging the event of surveillance VLAN.
Parameters	*enable* – Enable the logging machanism *disable* – Disable the logging mechanism
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable logging for sureveillance VLAN feature:

```
DGS-1210-28MP:5# config surveillance_vlan log state enable
Command: config surveillance_vlan log state enable

Success.
```

config surveillance_vlan onvif_discover_port

Purpose	To configure the discovery port of ONVIF (Open Network Video Interface Forum) device.
Syntax	**config surveillance_vlan onvif_discover_port {554 | <integer (1025-65535)>}**
Description	To configure the discovery port of ONVIF (Open Network Video Interface Forum) device.
Parameters	*544* – Default port <*interger 1025-65535*> – Range port number can be configured
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the port ONVIF discovery:

```
DGS-1210-28MP:5# config surveillance_vlan onvif_discover_port 1300
Command: config surveillance_vlan onvif_discover_port 1300

Success.
```

```
DGS-1210-28MP:5#
```

config surveillance_vlan oui

Purpose	To specifiy the particular OUI (Organization Unique Indentifier) values for surveillance VLAN auto detection feature.
Syntax	**config surveillance_vlan oui {add | delete} <macaddr> <macmask> [component_type {vms | vms_client | video_encoder | network_storage | other} description <desc (32)>]**
Description	To specifiy the particular OUI (Organization Unique Indentifier) values for surveillance VLAN auto detection feature. The OUI can be determined as range list by configuring MAC mask.
Parameters	<*macaddr*> - To specify the MAC address either by XX:XX:XX:XX:XX:XX or XX-XX-XX-XX-XX-XX format <*macmask*> - To specify the mask of MAC address indentified component type – type of connection device description <descr 32> - User defined description for specified OUI
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To specifiy the particular OUI (Organization Unique Indentifier) values for surveillance VLAN auto detection feature:

```
DGS-1210-28MP:5# config surveillance_vlan oui add 00:12:34:56:78:90 ff:ff:ff:ff:
ff:ff
Command: config surveillance_vlan oui add 00:12:34:56:78:90 ff:ff:ff:ff:ff:ff


Success.
```

config surveillance_vlan ports

Purpose	To change the the state of auto detection feature in surveillance VLAN.
Syntax	**config surveillance_vlan ports <portlist> state [enable | disable]**
Description	To change the the state of auto detection feature in Voice VLAN.
Parameters	<*portlist*> − A port, range of ports which would configured for Voice VLAN auto detection state.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To turn of surveillance VLAN on specific port:

```
DGS-1210-28MP:5# config surveillance_vlan ports 1 st en
Command: config surveillance_vlan ports 1 state enable


Success.
```

```
DGS-1210-28MP:5#
```

config surveillance_vlan onvif_ipc

Purpose	To manually congiure IP camera information in surveillance VLAN.
Syntax	**config surveillance_vlan onvif_ipc <ip_addr> [mac <macaddr> | description <desc (32)> | state {enable | disable}]**
Description	To manually congiure IP camera information in surveillance VLAN.
Parameters	*<ip_addr>* − IP address of the IP camera. *mac <macaddr>* - MAC address option *description <desc 32>* - Description string. Supports up 32 characters. *state {enable | disable}* – Specify the state of particular IP camera
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure IPC in surveillance VLAN:

```
DGS-1210-28MP:5# config surveillance_vlan onvif_ipc 10.1.1.1 mac 00:00:00:00:00:01
state enable
Command: config surveillance_vlan onvif_ipc 10.1.1.1 mac 00:00:00:00:00:01 state
enable

Success.

DGS-1210-28MP:5#
```

config surveillance_vlan onvif_nvr

Purpose	To manually congiure Network Video Recorder information in surveillance VLAN.
Syntax	**config surveillance_vlan onvif_nvr <ip_addr> [mac <macaddr> | description <desc (32)>]**
Description	To manually Network Vedio Recorder information in surveillance VLAN.
Parameters	*<ip_addr>* − IP address of the IP camera. *mac <macaddr>* - MAC address option *description <desc 32>* - Description string. Supports up 32 characters.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure NVR in surveillance VLAN:

```
DGS-1210-28MP:5# config surveillance_vlan onvif_nvr 10.1.1.2 description NVR-DLI
NK
Command: config surveillance_vlan onvif_nvr 10.1.1.2 description NVR-DLINK
Success.

DGS-1210-28MP:5#
```

show surveillance_vlan onvif_ipc_port

Purpose	To display IP camera information in surveillance VLAN.
Syntax	**show surveillance_vlan onvif_ipc [<portlist>] {brief | detail}**
Description	To display IP camera information in surveillance VLAN.
Parameters	*<portlist>* −Specify a port or a range of ports. *{brief | detail}* – Options for information display
Restrictions	None.

Example usage:

To display IPC in surveillance VLAN:

```
DGS-1210-28MP:5# show surveillance_vlan onvif_ipc_ports 1 brief
Command: show surveillance_vlan onvif_ipc_ports 1 brief


Total Entries      : 0

DGS-1210-28MP:5#
```

show surveillance_vlan onvif_nvr_port

Purpose	To display NVR information in surveillance VLAN.
Syntax	**show surveillance_vlan onvif_nvr [<portlist>] [ipc_list]**
Description	To display nvr information in surveillance VLAN.
Parameters	*<portlist>* −Specify a port or a range of ports. *[ipc_list]* – Specify the particular device
Restrictions	None.

Example usage:

To display NVR in surveillance VLAN:

```
DGS-1210-28MP:5# show surveillance_vlan onvif_nvr_ports 1
Command: show surveillance_vlan onvif_ipc_ports 1


Total Entries      : 0

DGS-1210-28MP:5#
```

show surveillance_vlan

Purpose	To display information of surveillance VLAN.
Syntax	**show surveillance_vlan [{ oui | ports [<portlist>] | device [ports <portlist>] }]**
Description	To display information of surveillance VLAN.
Parameters	*<portlist>* −Specify a port or a range of ports. *oui* – Specify the particular OUI

Restrictions	None.

Example usage:

To display information of surveillance VLAN:

```
DGS-1210-28MP:5# show surveillance_vlan
Command: show surveillance_vlan

Surveillance VLAN State   Enabled
VLAN ID                   5
VLAN Name                 VLAN5
Priority                  6
Aging Time                30
ONVIF Discover Port       1300
Log State                 Enabled

DGS-1210-28MP:5#
```

19

Q-IN-Q COMMANDS

The Link Aggregation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable qinq	
disable qinq	
show qinq	{ports [<portlist> | inner_tpid]}
config qinq ports	[<portlist> | all] [role [nni | uni] | outer_tpid <hex 0x1 - 0xffff> | add_inner_tag <hex 0x1-0xffff> | missdrop [enable | disable]]
config qinq inner_tpid	<hex 0x1-0xffff>
create vlan_translation	ports <portlist> [add | replace] cvid <vidlist> svid <vlanid 1-4094> {priority <priority 0-7>}
show vlan_translation	{cvid <vidlist>}
delete vlan_translation	ports [<portlist> | all] {cvid [<vidlist> | all]}

Each command is listed in detail, as follows:

enable qinq	
Purpose	To enable the Q-in-Q mode.
Syntax	**enable qinq**
Description	The **enable qinq** command creates a used to enable the Q-in-Q mode. When Q-in-Q is enabled, all network port roles will be NNI port and their outer TPID will be set to 88a8. All existing static VLANs will run as SP-VLAN. All dynamically learned L2 address will be cleared. GVRP and STP need to be disabled manually. If you need to run GVRP on the Switch, firstly enable GVRP manually. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DGS-1210-28MP:5# enable qinq
Command: enable qinq


Success.
DGS-1210-28MP:5#
```

disable qinq

Purpose	To disable the Q-in-Q mode.
Syntax	**disable qinq**
Description	The **disable qinq** command creates a used to disable the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled. If you need to run GVRP on the Switch, firstly enable GVRP manually. All existing SP-VLANs will run as static 1Q VLANs. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DGS-1210-28MP:5# disable qinq
Command: disable qinq


Success.
DGS-1210-28MP:5#
```

show qinq

Purpose	To show global Q-in-Q and port Q-in-Q mode status.
Syntax	**show qinq {ports [<portlist> | inner_tpid]}**
Description	The **show qinq** command is used to show the global Q-in-Q status, including: port role in Q-in-Q mode and port outer TPID.
Parameters	*<portlist>* - Specifies a range of ports to be displayed. If no parameter is specified, the system will display all Q-in-Q port information. *Inner_tpid* – Specifies the inner tpid to be showed.
Restrictions	None.

Example usage:

To show the Q-in-Q status for ports 1:

```
DGS-1210-28MP:5# show qinq ports 1
Command: show qinq ports 1

Port ID:  1
-------------------------------------------------------
  Role:              UNI
  Miss Drop:         Disabled
  Outer Tpid:        0x8100
  Add Inner Tag:     Disabled
-------------------------------------------------------
```

```
DGS-1210-28MP:5#
```

config qinq ports

Purpose	Used to configure Q-in-Q ports.
Syntax	**config qinq ports [<portlist> | all] [role [nni | uni] | outer_tpid <hex 0x1 - 0xffff> | add_inner_tag <hex 0x1-0xffff> | missdrop [enable | disable]]**
Description	The **config qinq ports** command is used to configure the port level setting for the Q-in-Q VLAN function. This setting is not effective when the Q-in-Q mode is disabled.
Parameters	*<portlist>* - A range of ports to configure. *all* – Specifies all ports to be configure. *role* - Port role in Q-in-Q mode, it can be UNI port or NNI port. *outer_tpid* - TPID in the SP-VLAN tag. *add_inner_tag* - For inner tag packets. *missdrop* – By enabling the parameter, the VLAN translation will performed on the port. The setting is disabled by default.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure port list 1 to 4 as NNI port, set outer TPID to 0x88a8:

```
DGS-1210-28MP:5# config qinq ports 1-3 role nni outer_tpid 0x88a8
Command: config qinq ports 1-3 role nni outer_tpid 0x88a8

Success.

DGS-1210-28MP:5#
```

config qinq inner_tpid

Purpose	Used to configure Q-in-Q inner TPID of the Switch.
Syntax	**config qinq inner_tpid <hex 0x1-0xffff>**
Description	The **config qinq inner_tpid** command is used to configure the inner TPID for port.
Parameters	<hex 0x1-0xffff> - Specifies the inner-TPID of a port.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the inner TPID to 0x88a8:

```
DGS-1210-28MP:5# config qinq inner_tpid 0x88a8
Command: config qinq inner_tpid 0x88a8

Success.

DGS-1210-28MP:5#
```

create vlan_translation

Purpose	To create a VLAN translation rule that will be added as a new rule or replace a current rule.
Syntax	**create vlan_translation ports <portlist> [add | replace] cvid <vidlist> svid <vlanid 1-4094> {priority <priority 0-7>}**
Description	The **create vlan_translation cvid** command is used to create a VLAN translation rule to add to or replace the outgoing packet which is single S-tagged (the C-VID changes to S-VID and the packet's TPID changes to an outer TPID).
Parameters	*ports <portlist>* - A range of ports to be configure. *cvid* – C-VLAN ID of packets that ingress from a UNI port. *svid* – The S-VLAN ID that replaces the C-VLAN ID or is inserted in the packet. <*vlanid 1-4094*> – A VLAN ID between 1 and 4094. *priority <priority 0-7>* - Configure the priority of specified ports.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a VLAN translation on the Switch:

```
DGS-1210-28MP:5# create vlan_translation add cvid 2 svid 2
Command: create vlan_translation add cvid 2 svid 2



Success.
DGS-1210-28MP:5#
```

show vlan_translation

Purpose	To display the current VLAN translation rules on the Switch.
Syntax	**show vlan_translation {cvid <vidlist>}**
Description	The **show vlan_translation cvid** command display the current VLAN translation cvid on the Switch.
Parameters	<*vidlist*> − The Q-in-Q translation rules for the specified C-VID list.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To display the VLAN translation cvid on the Switch:

```
DGS-1210-28MP:5# show vlan_translation cvid 1
Command: show vlan_translation cvid 1

Port   CVID      SPVID     Action    Priority
-------  --------  ----------  ----------  -------------

 Total Entries: 0

DGS-1210-28MP:5#
```

delete vlan_translation ports	
Purpose	To delete VLAN translation rules.
Syntax	**delete vlan_translation ports [<portlist> | all] {cvid [<vidlist> | all]}**
Description	The **delete vlan_translation cvid** command is used to delete VLAN translation rules.
Parameters	*ports* <*portlist*> - A range of ports to be deleted. <*vidlist*> - Specifies C-VID rules in VLAN translation. *all* – Specifies all C-VID rules to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete all C-VID VLAN translation rules:

```
DGS-1210-28MP:5# delete vlan_translation cvid all
Command: delete vlan_translation cvid all


Success.
DGS-1210-28MP:5#
```

20

BASIC IP COMMANDS

The Basic IP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config ipif system	[dhcp | dhcp_option12 {clear_hostname | hostname <hostname 63> state [enable | disable] } | ipaddress [<network_address> gateway <ipaddr>] | [ipv6 ipv6address <ipv6networkaddr>] | [dhcpv6_client [enable | disable]]]
show ipif	
config dhcp_client retry_time	<value 5-120>

Each command is listed in detail, as follows:

config ipif System	
Purpose	To configure the DHCPv6 client state for the interface.
Syntax	**config ipif System [dhcp | dhcp_option12 {clear_hostname | hostname <hostname 63> state [enable | disable] } | ipaddress [<network_address> gateway <ipaddr>] | [ipv6 ipv6address <ipv6networkaddr>] | [dhcpv6_client [enable | disable]]]**
Description	The **config ipif system** command is used to configure the DHCPv6 client state for one interface.
Parameters	*system* − The IP interface name to be configured. The default IP Interface name on the Switch is 'System'. All IP interface configurations done are executed through this interface name. *dhcp* − Specifies the DHCP protocol for the assignment of an IP address to the Switch to use for the DHCP Protocol. *hostname <hostname 63>* – Specifies the host name of DHCP. *ipaddress <network_address>* − IP address and netmask of the IP interface to be created. The address and mask information may be specified by using the traditional format (for example, 10.1.2.3/255.0.0.0 or in CIDR format, 10.1.2.3/16). *gateway <ipaddr>* − IP address of gateway to be created. *state [enable | disable]* − Enables or disables the IP interface. ipv6 ipv6address <ipv6networkaddr> − IPv6 network address: The address should specify a host address and length of network prefix. There can be multiple V6 addresses defined on an interface. Thus, as a new address is defined, it is added on this IP interface. *dhcpv6_client [enable | disable]* − Enable or disable the DHCPv6 client state of the interface.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the DHCPv6 client state of the System interface to enabled:

```
DGS-1210-28MP:5# config ipif System dhcpv6_client enable
Command: config ipif System dhcpv6_client enable


Success.
DGS-1210-28MP:5#
```

show ipif

Purpose	To display the configuration of an IP interface on the Switch.
Syntax	**show ipif**
Description	The **show ipif** command displays the configuration of an IP interface on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display IP interface settings:

```
DGS-1210-28MP:5#  show ipif
Command: show ipif


IP Setting Mode                 : Static
IP Address                      : 10.90.90.90
IP Subnet Mask                  : 255.0.0.0
IP Default Gateway              : 0.0.0.0
Interface Admin State           : Enabled
DHCPv6 Client State             : Disabled
IPv6 Link-Local Address         :
IPv6 Global Unicast Address     :
DHCP Option12 State             : Disabled
DHCP Option12 Host Name         : DGS-1210-28MP
DHCP retry time                 : 7
DHCP retry interval             : 5
IPv4 State                      : Enabled
IPv6 State                      : Enabled
DGS-1210-28MP:5#
```

config dhcp_client retry_time

Purpose	To configure the retry timer when system interface running in DCHP client mode.
Syntax	**config dhcp_client**
Description	The **show ipif** command is used to adjust the retry time period when system interface running as DHCP client mode. The measure unit is minute.
Parameters	None.

Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the retry time when system running in DHCP client mode:

```
DGS-1210-28MP:5# config dhcp_client retry_time 5
Command: config dhcp_client retry_time 5


Success.

DGS-1210-28MP:5#
```

21

MAC NOTIFICATION COMMANDS

The MAC Notification commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
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	{ ports [portlist | all] }

Each command is listed in detail, as follows:

enable mac_notification	
Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	**enable mac_notification**
Description	The **enable mac_notification** command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To enable MAC notification without changing basic configuration:

```
DGS-1210-28MP:5# enable mac_notification
Command: enable mac_notification

Success.
DGS-1210-28MP:5#
```

disable mac_notification	
Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	**disable mac_notification**
Description	The **disable mac_notification** command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To disable MAC notification without changing basic configuration:

```
DGS-1210-28MP:5# disable mac_notification
Command: disable mac_notification

Success.
DGS-1210-28MP:5#
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	**config mac_notification [interval <int 1-2147483647> | historysize <int 1-500>]**
Description	The **config mac_notification** command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*interval <int 1-2147483647>* − The time in seconds between notifications. The user may choose an interval between 1 and 2147483647 seconds. *historysize <1-500>* − The maximum number of entries listed in the history log used for notification.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To configure the Switch's MAC address table notification global settings:

```
DGS-1210-28MP:5# config mac_notification interval 1
Command: config mac_notification interval 1

Success.
DGS-1210-28MP:5#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist > | all] [enable | disable]**
Description	The **config mac_notification ports** command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist >* − Specifies a port or range of ports to be configured. *all* – Entering this command will set all ports on the system. *[enable* | *disable]* – These commands will enable or disable MAC address table notification on the Switch.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-1210-28MP:5# config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.
```

```
DGS-1210-28MP:5#
```

show mac_notification

Purpose	Used to display the Switch's MAC address table notification global settings.
Syntax	**show mac_notification**
Description	The **show mac_notification** command is used to display the the configuration of MAC notification.
Parameters	None.
Restrictions	None.

Example usage:

To view the Switch's MAC address table notification global settings:

```
DGS-1210-28MP:5# show mac_notification
Command: show mac_notification

Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1
DGS-1210-28MP:5#
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings.
Syntax	**show mac_notification ports <portlist >**
Description	The **show mac_notification ports** command is used used to display the the configuration of MAC notification in port basis.
Parameters	*<portlist>* − Specify a port or a range of ports. Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None.

Example usage:

To display port's MAC address table notification status settings:

```
DGS-1210-28MP:5#  show mac_notification ports 1-3
Command: show mac_notification ports 1-3

Port #  MAC Address Table Notification State
--------  ------------------------------------
1         Disabled
2         Disabled
3         Disabled
```

```
DGS-1210-28MP:5#
```

22

IGMP SNOOPING COMMANDS

The IGMP Snooping commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable igmp_snooping	{multicast_vlan | forward_mcrouter_only}
disable igmp_snooping	{multicast_vlan | forward_mcrouter_only}
config igmp_snooping	[vlan_name <string 32> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | fast_leave [enable | disable] | | report_suppression [enable | disable] | state [enable | disable] | proxy_reporting [state {enable | disable} source_ip <ipaddr>]]
config igmp_snooping querier	[vlan_name <string 32> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}
show igmp_snooping	{vlan <vlan_name 20>}
create igmp_snooping multicast_vlan	<vlan_name 20> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 20> [add | delete] [member_port <portlist > | source_port <portlist > | tag_member_port <portlist >] state [enable | disable] {replace_source_ip [none | <ipaddr>}
delete igmp_snooping multicast_vlan	[<vlan_name 20> | all]
show igmp_snooping multicast_vlan	<vlan_name 20>
config igmp_snooping multicast_vlan_group	<vlan_name 20> [ip | ipv6] [add | delete] ipv4_range <mcast_address_range>
show igmp_snooping multicast_vlan_group	<vlan_name 20>
config router_ports	[vlan_name <string 20> | vlanid <vidlist 1-4094> | all] [add | delete] <portlist >
config router_port s_forbidden	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
show router_port	{vlan <vlan_name 20> | vlanid <vidlist 1-4094> | static | dynamic | forbidden}
config igmp access_authentication ports	[<portlist> | all] state [enable | disable]
show igmp access_authentication ports	[<portlist> | all]
show igmp_snooping host	{group <ipaddr> | ports <portlist > | vlan <vlan_name 20> | vlanid <vidlist 1-4094>}

Command	Parameter
show igmp_snooping forwarding	{vlan <vlan_name 32> | vlanid <vidlist>}
show igmp_snooping group	[{vlan <vlan_name (32)> | vlanid <vidlist> | ports <portlist>}] [<ipaddr>] [data_driven]
config igmp_snooping data_driven_learning	[all | vlan_name <string 32> | vlanid <vidlist>] {state [enable | disable] aged_out [enable | disable]}
config igmp_snooping data_driven_learning	max_learned_entry <integer 1-1024>
clear igmp_snooping data_driven_group	[all | vlan_name <vlan_name 32> | vlanid < vidlist >] [all | MCGroupAddr <ipaddr>]
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_name <string (32)> | vlanid <vidlist> | ports <portlist>}
clear igmp_snooping statistics counter	
config igmp_snooping rate_limit	([state {enable | disable}] [rate <integer (1-199)>]

Each command is listed in detail, as follows:

enable igmp_snooping	
Purpose	To enable IGMP snooping or other sub-features on the Switch.
Syntax	**enable igmp_snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **enable igmp_snooping** command enables IGMP snooping or other sub-features on the Switch on the Switch.
Parameters	*{multicast_vlan* | *forward_mcrouter_only}* – Optional paratmeter for "multicast VLAN" and "forward to multicast router only".
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DGS-1210-28MP:5#  enable igmp_snooping
Command: enable igmp_snooping

Success.
DGS-1210-28MP:5#
```

disable igmp_snooping

Purpose	To disable IGMP snooping or other sub-features on the Switch.
Syntax	**disable igmp_snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **disable igmp_snooping** command enables IGMP snooping or other sub-features on the Switch on the Switch.
Parameters	*{multicast_vlan* | *forward_mcrouter_only}* – Optional paratmeter for "multicast VLAN" and "forward to multicast router only".
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DGS-1210-28MP:5#  disable igmp_snooping
Command: disable igmp_snooping

Success.
DGS-1210-28MP:5#
```

config igmp_snooping

Purpose	To configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping [vlan_name <string 32> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | fast_leave [enable | disable] | report_suppression [enable | disable] | state [enable | disable] | proxy_reporting [state {enable | disable} source_ip <ipaddr>]]**
Description	The **config igmp_snooping** command configures IGMP snooping on the Switch.
Parameters	*vlan_name* <*string 32*> − The name of the VLAN for which IGMP snooping is to be configured. *vlanid* <*vidlist*> − The VLAN id for which IGMP snooping is to be configured. *all* − Specifies all VLAN for which IGMP snooping is to be configured. *host_timeout* <*sec 130-153025*> − Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *router_timeout* <*sec 60-600*> − Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report. *fast_leave [enable* | *disable]* − Enables or disables the fast leave. *state [enable* | *disable]* − Enables or disables IGMP snooping for the specified VLAN. *proxy_reporting* **—**- Specifies the proxy reporting option *state* - Specifies the proxy reporting state. *enable* - Specifies that the proxy reporting option will be enabled. *disable* - Specifies that the proxy reporting option will be disabled.

	source_ip - Specifies the source IP address used. *<ipaddr>* - Enter the source IP address used here.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure the igmp snooping:

DGS-1210-28MP:5# config igmp_snooping vlanid 2 fast_leave enable host_timeout 130 leave_timer 2 report_suppression disable router_timeout 60 state enable

Command: config igmp_snooping vlanid 2 fast_leave enable host_timeout 130 leave_timer 2 report_suppression disable router_timeout 60 state enable

Success.

DGS-1210-28MP:5#

config igmp_snooping querier

Purpose	To configure IGMP snooping querier on the Switch.
Syntax	**config igmp_snooping querier [vlan_name <string 32> | vlanid <vidlist> | all] state [enable | disable] {querier_version [2 | 3] | last_member_query_interval <sec 1-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | max_response_time <sec 10-25>}**
Description	The **config igmp_snooping querier** command enables IGMP snooping querier on a specific VLAN.
Parameters	*vlan_name <string 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 20 characters can be used. *vlanid <vidlist>* − The VLAN id for which IGMP snooping is to be configured. *all* − Specifies all VLAN for which IGMP snooping is to be configured. *state [enable | disable]* − Enables/Disables IGMP Snooping Querier. *querier_version [2 | 3]* − Specifies the IGMP Querier version on the VLAN. *last_member_query_interval [sec 1-25]* − Specifies the IGMP last member query interval on the VLAN. *query_interval [sec 60-600]* − Specifies the IGMP query interval on the VLAN. *robustness_variable [value 2-255]* − Specifies the robustness on the VLAN. *max_response_time [sec 10-25]* − Specifies the max response time on the VLAN.
Restrictions	Only administrator, operator or power user-level users can issue this command.

Example usage:

To configure the igmp snooping:

DGS-1210-28MP:5# config igmp_snooping querier vlanid 2 state enable

Command: config igmp_snooping querier vlanid 2 state enable

```
Success .
DGS-1210-28MP:5#
```

show igmp_snooping

Purpose	To display IGMP snooping on the Switch.
Syntax	**show igmp_snooping {vlan <vlan_name 20>}**
Description	The **show igmp_snooping** command displays IGMP snooping on the Switch.
Parameters	*vlan <vlan_name 20>* − Displays the vlan for IGMP Snooping on the Switch.
Restrictions	None.

Example usage:

To display IGMP snooping on the Switch:

```
DGS-1210-28MP:5#  show igmp_snooping vlan default
Command: show igmp_snooping vlan default

IGMP Snooping Global State          : Enabled
Forward Router Only                 : Enabled


VLAN  Name                      : default
Host Timeout                    : 260
Router Timeout                  : 250
Query Interval                  : 125
Max Response Time               : 10
Robustness Value                : 2
Last Member Query Interval      : 2
Querier State                   : Disabled
State                           : Enabled
Fast Leave                      : Disabled
Version                         : 3

Total Entries: 1

DGS-1210-28MP:5#
```

create igmp_snooping multicast_vlan

Purpose	To create an IGMP snooping multicast VLAN on the Switch.
Syntax	**create igmp_snooping multicast_vlan <vlan_name 20> <vlanid 2-4094>**
Description	The **create igmp_snooping multicast_vlan** command creates an IGMP snooping multicast VLAN on the Switch.

Parameters	*vlan <vlan_name 20>* − The name of the VLAN for which IGMP snooping is to be created. Up to 32 characters can be used. <vlanid 2-4092> − The ID of the VLAN for which IGMP snooping is to be created. The range is from 2 to 4094.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a igmp snooping multicast VLAN:

```
DGS-1210-28MP:5# create igmp_snooping multicast_vlan mvln2 5
Command: create igmp_snooping multicast_vlan mvln2 5

Success.
DGS-1210-28MP:5#
```

config igmp_snooping multicast_vlan

Purpose	To configure IGMP snooping multicast VLAN on the Switch.
Syntax	**config igmp_snooping multicast_vlan <vlan_name 20> [add | delete] [member_port <portlist > | source_port <portlist > | tag_member_port <portlist >] state [enable | disable] {replace_source_ip [none | <ipaddr>]}**
Description	The **config igmp_snooping multicast_vlan** command enables IGMP snooping multicast VLAN on the Switch.
Parameters	*vlan <vlan_name 20>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *[add | delete] − Add or delete the specified multicast VLAN of IGMP snooping.* *member_port <portlist >* − Specifies a port or a range of ports to be the member port for the multicast VLAN of IGMP snooping. *source_port <portlist >* − Specifies a port or a range of ports to be the source port for the multicast VLAN of IGMP snooping. *tag_member_port <portlist >* − Specifies a port or a range of ports to be the tagged port for the multicast VLAN of IGMP snooping. *state [enable | disable]* − Enables/Disables IGMP Snooping multicast VLAN. *replace_source_ip [none | <ipaddr>]* – Specifies the replace source IP address.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-1210-28MP:5# config igmp_snooping multicast_vlan default state enable
Command: config igmp_snooping multicast_vlan default state enable

Success.
DGS-1210-28MP:5#
```

delete igmp_snooping multicast_vlan

Purpose	To remove an IGMP snooping multicast VLAN on the Switch.
Syntax	**delete igmp_snooping multicast_vlan [<vlan_name 20> | all]**
Description	The **delete igmp_snooping multicast_vlan** command removes IGMP snooping multicast VLAN on the Switch.
Parameters	*<vlan_name 20>* − Specify the multicast vlan name to be removed on the Switch. *[all]* – All multicast VLAN groups.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To remove the igmp snooping multicast VLAN 'rd1':

```
DGS-1210-28MP:5# delete igmp_snooping multicast_vlan rd1
Command: delete igmp_snooping multicast_vlan rd1

Success.
DGS-1210-28MP:5#
```

config igmp_snooping multicast_vlan_group

Purpose	To specify that IGMP snooping is to be configured for multicast vlan groups on the Switch.
Syntax	**config igmp_snooping multicast_vlan_group <vlan_name 20> [ip | ipv6] [add | delete] [<mcast_address_range> | all]**
Description	The **config igmp_snooping multicast_vlan_group** command specifies an IGMP snooping multicast VLAN group on the Switch.
Parameters	*vlan <vlan_name 20>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *[ip | ipv6]* − Specify the ip or ipv6 of multicast vlan group to be configured on the Switch. *[add | delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. *[<mcast_address_range> | all]* − Specify the address to be configured with the IGMP snooping multicast VLAN group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-1210-28MP:5#  config igmp_snooping multicast_vlan_group default
ip delete all
Command: config igmp_snooping multicast_vlan_group default ip delete
all

Success.
DGS-1210-28MP:5#
```

show igmp_snooping multicast_vlan

Purpose	To display the IGMP snooping multicast vlan table entries on the Switch.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 20>}**
Description	The **show igmp_snooping multicast_vlan** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 20>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the IGMP snooping multicast vlan information on the Switch:

```
DGS-1210-28MP:5# show igmp_snooping multicast_vlan mvln2
Command: show igmp_snooping multicast_vlan mvln2

Multicast VLAN Global State : Disabled

VLAN Name          : mvln2
VID                : 5
Member Ports       :
Tagged Member Ports :
Source Ports       :
Status             : Disabled
Replace Source IP  :
```

config igmp_snooping multicast_vlan_group

Purpose	To specify that IGMP snooping is to be configured for multicast vlan groups on the Switch.
Syntax	**config igmp_snooping multicast_vlan_group <vlan_name 32> [add | delete] ipv4_range <ipaddr> <ipaddr>**
Description	The **config igmp_snooping multicast_vlan_group** command specifies an IGMP snooping multicast VLAN group on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *[add | delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. *<ipaddr>* − Specify the IP address range to be configured with the IGMP snooping multicast VLAN group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-1210-28MP:5# config igmp_snooping multicast_vlan_group test add
ipv4_range 2
39.255.0.1 239.255.1.1
Command: config igmp_snooping multicast_vlan_group test add ipv4_range
```

```
239.255.0.1 239.255.1.1


Success.

DGS-1210-28MP:5#
```

show igmp_snooping multicast_vlan_group

Purpose	To display the IGMP snooping multicast vlan group table entries on the Switch.
Syntax	**show igmp_snooping multicast_vlan_group {<vlan_name 32>}**
Description	The **show igmp_snooping multicast_vlan_group** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To view the IGMP snooping multicast vlan group information on the Switch:

```
DGS-1210-28MP:5# show igmp_snooping multicast_vlan_group
Command: show igmp_snooping multicast_vlan_group

VLAN Name     VLAN ID    From                To
------------- ---------  ------------------  ------------------
test          2000       239.255.0.1         239.255.1.1

DGS-1210-28MP:5#
```

config router_ports

Purpose	To configure ports as router ports.
Syntax	**config router_ports [vlan_name <string 20> | vlanid <vidlist 1-4094> | all] [add | delete] <portlist >**
Description	The **config router_ports** command designates a range of ports as being connected to multicast-enabled routers. This ensures all packets with such a router as its destination will reach the multicast-enabled router − regardless of protocol, etc.
Parameters	*vlan_name <string 20>* − The name of the VLAN on which the router port resides. Up to 20 characters can be used. *vlanid <vidlist 1-4094>* − The VLAN id of the VLAN on which the router port resides. *all* − Specifies all ports on the Switch to be configured. *[add | delete]* – Specifies whether to add or delete ports defined in the following parameter <portlist>, to the router port function. *<portlist >* − A port or range of ports that will be configured as router ports.

Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To add a static router port:

```
DGS-1210-28MP:5#  config router_ports vlanid 12 add 2
Command: config router_ports vlanid 12 add 2

Success.
DGS-1210-28MP:5#
```

config router_ports_forbidden

Purpose	To deny ports becoming router ports.
Syntax	**config router_ports_forbidden [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config router_port_forbidden** command denies a range of ports access to multicast–enabled routers. This ensures all packets with such a router as its destination will not reach the multicast–enabled router − regardless of protocol, etc.
Parameters	*vlan_name <string 32>* − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *vlanid <vidlist>* − The VLAN id of the VLAN on which the router port resides. *all* − Specifies all ports on the Switch to be configured. *[add | delete]* – Specifies whether to deny ports defined in the following parameter <portlist>, to the router port function. *<portlist>* − A port or range of ports that will be denied access as router ports.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To deny router ports:

```
DGS-1210-28M:5# config router_ports_forbidden vlanid 2 add 10-12
Command: config router_ports_forbidden vlanid 2 add 10-12


Success.
DGS-1210-28MP:5#
```

show router_ports

Purpose	To display the currently configured router ports on the Switch.
Syntax	**show router_ports {vlan <vlan_name 32> | vlanid <vidlist> | static | dynamic | forbidden}**
Description	The **show router_ports** command displays the router ports currently configured on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *vlanid <vidlist>* − The ID of the VLAN on which the router port

	resides. *static* − Displays router ports that have been statically configured. *dynamic* − Displays router ports that have been dynamically learned. *forbidden* − Displays router ports that have been forbidden configured.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-1210-28MP:5# show router_ports
Command: show router_ports

VLAN Name            : default
Static router port   :
Dynamic router port  :
Forbidden router port :

Total Entries : 1
DGS-1210-28MP:5#
```

config igmp access_authentication ports

Purpose	To configure the IGMP access authentication on the Switch.
Syntax	**config igmp access_authentication ports [<portlist > | all] state [enable | disable]**
Description	The **config igmp access_authentication ports** command configures the IGMP access authentication on the Switch.
Parameters	*<portlist* > − A port or range of ports that will be configured as IGMP access authentication ports. *all* − Specify all ports to be configured as IGMP access authentication ports. *state[enable* | *disable]* − Specifies the state for the port to be disabled or enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure authentication port of IGMP:

```
DGS-1210-28MP:5# config igmp access_authentication ports all state enable
Command: config igmp access_authentication ports all state enable

Success !
DGS-1210-28MP:5#
```

show igmp access_authentication ports

Purpose	To display the IGMP access authentication configuration on the Switch.
Syntax	**show igmp access_authentication ports [<portlist > | all]**

Description	The **show igmp access_authentication** command displays the IGMP access authentication configuration on the Switch.
Parameters	*all* − Specifies all ports to be displayed. <*portlist* > − A port or range of ports to be displayed on the Switch.
Restrictions	None.

Example usage:

To display the IGMP access authentication:

```
DGS-1210-28MP:5#  show igmp access_authentication ports 1-3
Command: show igmp access_authentication ports 1-3

Port   Authentication State
---------------------------
1        : Enabled
2        : Enabled
3        : Enabled
DGS-1210-28MP:5#
```

show igmp_snooping host

Purpose	To display the IGMP snooping host table entries on the Switch.
Syntax	**show igmp_snooping host {ports <portlist> | group <ipaddr> | vlan <vlan_name 32> | vlanid <vidlist>}**
Description	The **show igmp_snooping host** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*ports* <*portlist*> − The ports of IGMP snooping host table information are to be displayed. *group* <*ipaddr*> − The IP address of IGMP snooping host table information are to be displayed. *vlan* <*vlan_name 32*> − The name of the VLAN for which IGMP snooping host table information is to be displayed. Up to 32 characters can be used. *vlanid* <*vidlist*> − The vid of the VLAN for which IGMP snooping host table information is to be displayed.
Restrictions	None.

Example usage:

To view the IGMP snooping host table on the Switch:

```
DGS-1210-28MP:5# show igmp_snooping host
Command: show igmp_snooping host

VLAN ID    Group                Port No      IGMP Host
 ------     ----------------------  ---------     ------------



Total Entries : 0

DGS-1210-28MP:5#
```

show igmp_snooping forwarding

Purpose	To display the IGMP snooping forwarding table entries on the Switch.
Syntax	**show igmp_snooping forwarding {vlan <vlan_name 32> | vlanid <vidlist>}**
Description	The **show igmp_snooping forwarding** command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping forwarding table information is to be displayed. Up to 32 characters can be used. *vlanid <vidlist>* − The vid of the VLAN for which IGMP snooping forwarding table information is to be displayed.
Restrictions	None.

Example usage:

To view the IGMP snooping forwarding table for VLAN 'Trinity':

```
DGS-1210-28MP:5# show igmp_snooping forwarding vlan default
Command: show igmp_snooping forwarding vlan default

VLAN Name      : Trinity
Multicast group : 224.0.0.2
MAC address    : 01-00-5E-00-00-02
Port Member    : 3,4
Total Entries  : 1

DGS-1210-28MP:5#
```

show igmp_snooping group

Purpose	To display the current IGMP snooping group configuration on the Switch.
Syntax	**show igmp_snooping group [vlan <vlan_name 32> | vlanid <vidlist>] <ipaddr> {data_driven}**
Description	The **show igmp_snooping group** command displays the current IGMP snooping group configuration on the Switch.
Parameters	*vlan <vlan_name 32>* − The name of the VLAN for which IGMP snooping group configuration information is to be displayed. Up to 32 characters can be used. *vlanid <vidlist>* − The ID of the VLAN for which IGMP snooping group configuration infor mation is to be displayed. *<ipaddr>* − The IP address of the VLAN for which IGMP snooping group configuration infor mation is to be displayed. *{data_driven}* − Specifies to display the data driven of IGMP snooping group.
Restrictions	None.

Example usage:

To show igmp snooping group:

```
DGS-1210-28MP:5# show igmp_snooping group vlan default
Command: show igmp_snooping group vlan default


Total Entries : 0

DGS-1210-28MP:5#
```

config igmp_snooping data_driven_learning

Purpose	To enable or disable the data driven learning of an IGMP snooping group. When data-driven learning is enabled for the VLAN, when the Switch receives the IP multicast traffic on this VLAN, an IGMP snooping group will be 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 be aged out or to be aged out by the aged timer. When 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 IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the aging out mechanism will follow the ordinary IGMP snooping entry.
Syntax	**config igmp_snooping data_driven_learning [all | vlan_name <string 32> | vlanid <vidlist>] {state [enable | disable] aged_out [enable | disable]}**
Description	The **config igmp_snooping data_driven_learning** command is used to enable or disable the data driven learning of an IGMP snooping group.
Parameters	*all* – Specifies all VLANs to be configured. *vlan_name <string 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *vlanid <vidlist>* − Specifies the VLAN ID to be configured. *state [enable | disable]* – Specifies to enable or disable the data driven learning of an IGMP snooping group. The defaule is enabled. *age_out [enable | disable]* – Specifies to enable or disable the aging out of the entry.By default, the state is enabled.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the data driven learning of an IGMP snooping group on the defaultVLAN:

```
DGS-1210-28MP:5# config igmp_snooping data_driven_learning vlan_name default
```

```
Command: config igmp_snooping data_driven_learning vlan_name default

Success.
DGS-1210-28MP:5#
```

config igmp_snooping data_driven_learning

Purpose	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 dada-driven groups. Traffic for the new groups will be dropped.
Syntax	**config igmp_snooping data_driven_learning max_learned_entry <integer 1-1024>**
Description	The **config igmp_snooping data_driven_learning** command is used to configure the maximum number of groups that can be learned by data driven.
Parameters	*max_learned_entry <integer 1-1024>* – Specifies the maximum number of groups that can be learned by data drive. This value must be between 1 and 1024, and the suggested default setting is 56.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To set the maximum number of groups that can be learned by data driven:

```
DGS-1210-28MP:5# config igmp_snooping data_driven_learning max_learned_entry 50
Command: config igmp_snooping data_driven_learning max_learned_entry 50

Success.
DGS-1210-28MP:5#
```

clear igmp_snooping data_driven_group

Purpose	To clear the IGMP snooping group learned by data drive.
Syntax	**clear igmp_snooping data_driven_group [all | vlan_name <vlan_name 32> | vlanid <vidlist>] [all | MCGroupAddr <ipaddr>]**
Description	The **config igmp_snooping data_driven_learning** command is used to delete the IGMP snooping group learned by data drive. Note that this commands is currently only for layer 2 switches.
Parameters	*all* − Delete all data driven entries. *vlan_name <vlan_name 32>* − The name of the VLAN for which IGMP snooping is to be configured. Up to 32 characters can be used. *vlanid* <vidlist> − Specify the vlan id of the IGMP snooping data driven group on the Switch. <ipaddr> - Specifies the IP address.
Restrictions	Only administrator, operator or power user-level users can issue this

	command.

Example usage:

To clear the igmp snooping data driven group on the Switch:

```
DGS-1210-28MP:5# clear igmp_snooping data_driven_group all
Command: clear igmp_snooping data_driven_group all

Success.
DGS-1210-28MP:5#
```

create igmp_snooping static_group

Purpose	To create an IGMP snooping static group on the Switch.
Syntax	**create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	The **create igmp_snooping static_group** command allows you to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port from the member ports of a group. The statis group will only take effect when IGMP snooping is enabled on the VLAN. For those statis 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.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping statis group is to be created. Up to 32 characters can be used. <*vlanid_list*> − The ID of the VLAN for which IGMP snooping static group is to be created. The range is from 2 to 4094. <*ipaddr*> − Specify the static group address for which IGMP snooping to be created.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a igmp snooping static group 226.1.1.1 for VID 1:

```
DGS-1210-28MP:5# create igmp_snooping static_group vlanid 1 226.1.1.1
Command: create igmp_snooping static_group vlanid 1 226.1.1.1

Success.
DGS-1210-28MP:5#
```

config igmp_snooping static_group

Purpose	To configure the current IGMP snooping static group on the Switch.
Syntax	**config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>**

Description	The **config igmp_snooping static_group** command is used to add or delete ports to /from the given static group.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping static group is to be configured. Up to 32 characters can be used. *[add	delete]* − Specify whether to add or delete ports defined in the following parameter <ipaddr>. *<ipaddr>* − Specify the IP address to be configured with the IGMP snooping static group.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To add port 5 to static group 226.1.1.1 on VID 1:

```
DGS-1210-28MP:5# config igmp_snooping static group vlanid 1 226.1.1.1 and 5


Success.
DGS-1210-28MP:5#
```

delete igmp_snooping static_group

Purpose	To delete the current IGMP snooping static group on the Switch.
Syntax	**delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	The **delete igmp_snooping static_group** command is used to delete an IGMP snooping statie group will not affect the IGMP snooping dynamic member ports of a group.
Parameters	*<vlan_name 32>* − The name of the VLAN for which IGMP snooping statis group is to be created. Up to 32 characters can be used. *<vlanid_list>* − The ID of the VLAN for which IGMP snooping static group is to be created. The range is from 2 to 4094. *<ipaddr>* − Specify the static group address for which IGMP snooping to be deleted.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete a static group 226.1.1.1 on VID 1:

```
DGS-1210-28MP:5# delete igmp_snooping static_group vlanid 1 226.1.1.1
Command: delete igmp_snooping static_group vlanid 1 226.1.1.1


Success.
DGS-1210-28MP:5#
```

show igmp_snooping static_group

Purpose	To display the IGMP snooping static group information on the

	Switch.
Syntax	show igmp_snooping **statis_group vlan <vlan_name 32> | vlanid <vlanid_list> | <ipaddr>}**
Description	The show igmp_snooping **statis_group** command displays the IGMP snooping static group information on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping static group to be displayed. <*vlanid_list*> − The VLAN id of IGMP snooping static group to be displayed. <*ipaddr*> − Specify the IP address of IGMP snooping static group to be displayed.
Restrictions	None.

Example usage:

To display the IGMP snooping static group information on the Switch:

```
DGS-1210-28MP:5# show igmp_snooping static_group vlan default
Command: show igmp_snooping static_group vlan default


 VLAN ID/Name     IP Address     Static Member Ports
 ----------------------  ---------------  ---------------------------------
 1     default          226.1.1.1          None

Total Entries : 1

DGS-1210-28MP:5#
```

show igmp_snooping statistic counter

Purpose	To display statistic for IGMP management packets in variable filter.
Syntax	**show igmp_snooping statistic counter {vlan_name <string (32)> | vlanid <vidlist> | ports <portlist>}**
Description	The **show igmp_snooping statistic counter** command can print the counter for all IGMP management packets in different filter basis.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping static group to be displayed. <*vlanid_list*> − The VLAN id of IGMP snooping static group to be displayed. <*ipaddr*> − Specify the IP address of IGMP snooping static group to be displayed.
Restrictions	None.

Example usage:

To display counter for IGMP packets in VLAN named “test”:

```
DGS-1210-28MP:5# show igmp_snooping statistic counter vlan_name test
Command: show igmp_snooping statistic counter vlan_name test
```

```
VLAN  Name         test
-------------------------------------------------
Group Number       0

Receive Statistics
   Query
      IGMP v1 Query          :0
      IGMP v2 Query          :0
      IGMP v3 Query          :0
      Total                  :0

   Report & Leave
      IGMP v1 Report         :0
      IGMP v2 Report         :0
      IGMP v3 Report         :0
      IGMP v2 leave          :0
      Total                  :0

Transmit Statistics
   Query
      IGMP v1 Query          :0
```

clear igmp_snooping statistic counter

Purpose	To clear statistic for IGMP management packets in variable filter.
Syntax	**clear igmp_snooping statistic counter**
Description	The **clear igmp_snooping statistic counter** command can clear the counter.
Parameters	None.
Restrictions	None.

Example usage:

To clear counter for IGMP packets:

```
DGS-1210-28MP:5# clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter

DGS-1210-28MP:5#
```

cofig igmp_snooping rate_limit

Purpose	To limit the rate of IGMP packets forwarded to CPU.
Syntax	**config igmp_snooping rate_limit ([state {enable | disable}] [rate <integer (1-200)>])**
Description	The **config igmp_snooping rate_limit** command can limit the rate of IGMP packets forwarded to CPU.
Parameters	*state {enable* | *disable*} – Determine the state of this IGMP packet

	filter. *rate <integer (1-200)>* – Specify the filter rate
Restrictions	Only administrator level users can issue this command.

Example usage:

To configure the rate of IGMP packets forwarded to CPU:

```
DGS-1210-28MP:5# config igmp_snooping rate_limit rate 200
Command: config igmp_snooping rate_limit rate 200


Success.
```

23

MLD SNOOPING COMMANDS

The MLD Snooping commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable mld_snooping	{multicast_vlan | forward_mcrouter_only}
disable mld_snooping	{multicast_vlan | forward_mcrouter_only}
config mld_snooping	[vlan_name < string 32> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-153025> | leave_timer <sec 1-25> | report_suppression [enable | disable] | router_timeout <sec 60-600> | state [enable | disable]}
config mld_snooping querier	[vlan_name <string 32> | vlanid <vidlist> | all] [last_listener_query_interval <sec 1-25> | max_response_time <sec 10-25> | query_interval <sec 60-600> | robustness_variable | state [enable | disable] | version <value 1-2>]
show mld snooping	[vlan_name <string 32> | vlanid <vidlist> | all]
create mld_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config mld_snooping multicast_vlan	<vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr>}
delete mld_snooping multicast_vlan	[<vlan_name 32> | all]
show mld_snooping multicast_vlan	<vlan_name 32>
config mld_snooping multicast_vlan_group	<vlan_name 32> [add | delete] ipv6_range <ipv6_mcast_addr> <ipv6_mcast_addr>
show mld_snooping multicast_vlan_group	{<vlan_name 32>}
config mld_snooping mrouter_ports	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
config mld_snooping mrouter_ports_forbidden	[vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>
show mld_snooping mrouter_ports	[vlan_name <string 32> | vlanid <vidlist> | all] [dynamic | static | forbidden]
show mld_snooping host	{group <ipv6_addr> | ports <portlist > | vlan <vlan_name 20> | vlanid <vidlist 1-4094>}
show mld_snooping forwarding	{vlan <vlan_name 32> | vlanid <vidlist> | all}
show mld_snooping group	[{vlan <vlan_name (32)> | vlanid <vidlist> | ports <portlist>}] [<ipv6_addr>] [data_driven]
config mld_snooping data_driven_learning	[all | vlan_name <string 32> | vlanid <vidlist>] ({state [enable | disable]} {aged_out [enable | disable]} {expiry_time <sec (130-153025)>})

Command	Parameter
config mld_snooping data_driven_learning	max_learned_entry <integer 1-1024>
clear mld_snooping data_driven_group	[all | vlan_name <vlan_name 32> | vlanid < vidlist >] [all | MCGroupAddr <ipv6_addr>]
show mld_snooping statistic counter	{vlan_name <string (32)> | vlanid <vidlist> | ports <portlist>}
clear mld_snooping statistics counter	

Each command is listed in detail, as follows:

enable mld_snooping

Purpose	To enable MLD snooping on the Switch.
Syntax	**enable mld snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **enable mld snooping** command enables MLD snooping on the Switch.
Parameters	*{multicast_vlan* | *forward_mcrouter_only}* − Enables the multicast VLAN or forward mcrouter for MLD Snooping on the Switch.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To enable the MLD snooping:

```
DGS-1210-28MP:5# enable mld_snooping
Command: enable mld_snooping


Success.
DGS-1210-28MP:5#
```

disable mld_snooping

Purpose	To disable MLD snooping on the Switch.
Syntax	**disable mld snooping {multicast_vlan | forward_mcrouter_only}**
Description	The **disable mld snooping** command disables MLD snooping on the Switch.
Parameters	*{multicast_vlan* | *forward_mcrouter_only}* − Disables the multicast VLAN or forward mcrouter for MLD Snooping on the Switch.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To disable the MLD snooping:

```
DGS-1210-28MP:5# disable mld_snooping
Command: disable mld_snooping
```

```
Success.
DGS-1210-28MP:5#
```

config mld_snooping

Purpose	To configure mld snooping.
Syntax	**config mld_snooping [vlan_name < string 32> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-153025> | leave_timer <sec 1-25> | report_suppression [enable | disable] | router_timeout <sec 60-600> | state [enable | disable]}**
Description	The **config mld_snooping** command defines mld snooping on the VLAN.
Parameters	*vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. vlanid <vidlist> – Specifies that the mld snooping applies only to this VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *fast_done [enable | disable]* – Specifies the fast down to be enabled or disabled. *host_timeout <sec 130-153025>* – Specifies the maximum amount of time a host can be a member of a multicast group without the Switch receiving a host membership report. The default is 260 seconds. *leave_timer <sec 1-25>* – Specifies the maximum amount of time a host can be a member of a multicast group after sending a done timer membership report. The default is 10 seconds. *report_suppression [enable | disable]* – Specifies the report suppression to be enabled or disabled. *router_timeout <sec 60-600>* – Specifies the maximum amount of time a route can be a member of a multicast group without the Switch receiving a host membership report done timer. The default is 300 seconds. *state [enable | disable]*– Allows the user to enable or disable MLD snooping for the specified VLAN.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure mld snooping:

```
DGS-1210-28MP:5# config mld_snooping vlan_name default fast_done disable
host_timeout 130 leave_timer 3 router_timeout 60 state enable
Command: config mld_snooping vlan_name default fast_done disable
host_timeout 130 leave_timer 3 router_timeout 60 state enable

Success.
DGS-1210-28MP:5#
```

config mld_snooping querier

Purpose	Used to configure the timers and settings for the MLD snooping querier for the Switch.
Syntax	**config mld_snooping querier [vlan_name <string 32> | vlanid <vidlist> | all] [last_listener_query_interval <sec 1-25> | max_response_time <sec 10-25> | query_interval <sec 60-600> | robustness_variable <value 2-255> | state [enable | disable] | version <value 1-2>]**
Description	The **config mld_snooping querier** command allows users to configure the time between general query transmissions, the maximum time to wait for reports from listeners and the permitted packet loss guaranteed by MLD snooping.
Parameters	*vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *last_listener_query_interval <sec 1-25>* – The maximum amount of time to be set between group-specific query messages. This interval may be reduced to lower the amount of time it takes a router to detect the loss of a last listener group. The user may set this interval between 1 and 25 seconds with a default setting of 1 second. *max_response_time <sec 10-25>* – The maximum time to wait for reports from listeners. The user may specify a time between 1 and 25 seconds with a default setting of 10 seconds. *query_interval <sec 60-600>* – Specifies the amount of time between general query transmissions. The user may specify a time between 1 and 65535 seconds with a default setting of 125 seconds. *robustness_variable <value 2-255>* – Provides fine-tuning to allow for expected packet loss on a subnet. The user may choose a value between 1 and 255 with a default setting of 2. If a subnet is expected to be lossy, the user may wish to increase this interval. *state [enable | disable]* – Enabling the querier state will set the Switch as a MLD querier and disabling it will set it as a Non-querier. The default setting is disabled. *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 forward from router ports or VLAN flooding. The value is between 1 and 2.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure MLD snooping querier:

DGS-1210-28MP:5#config mld_snooping querier all last_listener_query_interval 1 max_response_time 10 query_interval 60 robustness_variable 2 state disable version 1

Command: config mld_snooping querier all last_listener_query_interval 1 max_response_time 10 query_interval 60 robustness_variable 2 state disable version 1

```
Success.
DGS-1210-28MP:5#
```

config mld_snooping router_ports

Purpose	To enable mld mrouter ports.
Syntax	**config mld_snooping router_ports [vlan_name <string 20> | vlanid <vidlist 1-4094> | all] [add | delete] <portlist >**
Description	The **config mld_snooping router_ports** command defines a port that is connected to a multicast router port.
Parameters	*vlan_name <string 20>* – specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist 1-4094>* – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port. *delete* – Deletes a specified port to the mld snooping mrouter port. <*portlist* > – Defines the ports to be included from the mld snooping mrouter group.
Restrictions	Only administrator or operator–level users can issue this command Separate non–consecutive Ethernet ports with a comma and no spaces; use a hyphen to designate a range of ports. These ports are defined as connected to a multicast router.

Example usage:

To configure mld mrouter ports:

```
DGS-1210-28MP:5#  config mld_snooping router_ports vlanid 1 add 3
Command: config mld_snooping router_ports vlanid 1 add 3


Success.

DGS-1210-28MP:5#
```

show mld_snooping

Purpose	To display mld snooping settings on the Switch.
Syntax	**show mld_snooping [vlan <vlan_name 20> | vlanid <vidlist 1-4094> | all]**
Description	The **show mld_snooping** command displays a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters	*vlan <vlan_name 20>* – Displays that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist 1-4094>* – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that MLD snooping which configured for all VLANs on the Switch.

Restrictions	None.

Example usage:

To show the MLD snooping:

```
DGS-1210-28MP:5#  show mld_snooping vlan default
Command: show mld_snooping vlan default

MLD Snooping Global State          : Enabled


VLAN  Name                         : default
Host Timeout                       : 260
Router Timeout                     : 250
Query Interval                     : 125
Max Response Time                  : 10
Robustness Value                   : 2
Last Member Query Interval         : 2
Querier State                      : Disabled
State                              : Enabled
Fast Leave                         : Disabled
Version                            : 2

Total Entries: 1

DGS-1210-28MP:5#
```

create mld_snooping multicast_vlan

Purpose	To create an MLD multicast VLAN.
Syntax	**create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>**
Description	The **config mld_snooping multicast_vlan** command will create a MLD multicast_vlan. Multiple multicast VLANs can be configured. When creating MLD multicast VLAN, it cannot duplicate with the VLAN entries in the existing 802.1Q VLAN database. The MLD Multicast VLAN snooping function co-exists with the 1Q VLAN snooping function.
Parameters	*<vlan_name 32>* − The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 20 characters. *vlanid* – The VLAN ID of the multicast VLAN to be create. The range is 2-4094.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To create mld snooping multicast VLAN mv1:

```
DGS-1210-28MP:5# create mld_snooping multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.
```

```
DGS-1210-28MP:5#
```

config mld_snooping multicast_vlan

Purpose	To configure an MLD multicast VLAN.
Syntax	**config mld_snooping multicast_vlan <vlan_name 32> {[add | delete] [member_port <portlist> | [source_port <portlist> | untag_source_port <portlist>] | tag_member_port <portlist>] | state [enable | disable] | replace_source_ipv6 <ipv6addr> | remap_priority [<value 0-7> | none] { replace_priority}}**
Description	The **config mld_snooping multicast_vlan** command allows you to add an untagged member port, a tagged member port, a untagged source port and a tagged source port to the port list. The untagged member port and the untagged source port will automatically become the untagged members of the multicast VLAN, the tagged member port and the tagged source port will automatically become the tagged members of the multicast VLAN. To change the port list, the Switch will add or delete the port list that user entered, and update the previous port list. The member port list and source port list cannot overlap. However, the member port of one multicast VLAN can overlap with another multicast VLAN. Before configuring the multicast VLAN member port by using this command, the multicast VLAN must be created first.
Parameters	<*vlan_name 32*> − The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 20 characters. *member_port* – Adds a range of member ports to the multicast VLAN. They will become the untagged member port of the MLD multicast VLAN. *source_port* – Adds a range of source ports to the multicast VLAN. *untag_source_port* – Adds a range of untagged source ports to the multicast VLAN.The PVID of the untag source port will be automatically changed to the multicast VLAN. It shall be only one kind of source port, tag or untag for an ISM VLAN. *tag_member_port* – Specifies the tagged member port of the MLD multicast VLAN. *state* – enable or disable multicast VLAN for the chosen VLAN. *replace_source_ipv6* <*ipv6addr*> – With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before the forwarding of the packet, the source IP address in the join packet needs to be replaced by this IPv6 address. *remap_priority* – Associates the remap priority value (*0* to *7*) with the data traffic and is forwarded on the multicast VLAN. If *none* is specified, the packet's original priority will be used.The default setting is *none*.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To config MLD multicast VLAN mv1:

```
DGS-1210-28MP:5# config mld_snooping multicast_vlan mv1 add member_port 1,3 state enable
Command: config mld_snooping multicast_vlan mv1 add member_port 1,3 state enable
```

```
Success.
DGS-1210-28MP:5#
```

delete mld_snooping multicast_vlan

Purpose	To to delete an MLD muticast VLAN.
Syntax	**delete mld_snooping multicast_vlan [<vlan_name 32> | all]**
Description	The **delete mld_snooping multicast_vlan** command allows user to delete an MLD multicast VLAN.
Parameters	*[<vlan_name 32> | all]* – Specifies the name or all multicast VLAN to be deleted.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To delete a MLD multicast VLAN:

```
DGS-1210-28MP:5# delete mld_snooping multicast_vlan mv1
Command: delete mld_snooping multicast_vlan mv1

Success.
DGS-1210-28MP:5#
```

show mld_snooping multicast_vlan

Purpose	To to show the information of MLD multicast VLAN.
Syntax	**show mld_snooping multicast_vlan <vlan_name 32>**
Description	The **show mld_snooping multicast_vlan** command allows user to show the information of an MLD multicast VLAN.
Parameters	*<vlan_name 32>* – specifies that the mld snooping applies only to this previously created VLAN.
Restrictions	None.

Example usage:

To show MLD multicast VLAN:

```
DGS-1210-28MP:5# show mld_snooping multicast_vlan mv1
Command: show mld_snooping multicast_vlan mv1

Multicast VLAN Global State : Enabled
DGS-1210-28MP:5#
```

config mld_snooping multicast_vlan_group

Purpose	To bind a multicast group profile to a multicast VLAN. The binding profile will affect the group joined to the multicast VLAN.
Syntax	**config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] ipv6_range <ipv6addr> <ipv6addr>**
Description	After binding a profile to a multicast VLAN, when a multicast group attempt to join this multicast VLAN member port, the group cannot

	join this multicast VLAN if the group does not belong to the range of binding profile.
Parameters	*<vlan_name 32>* − The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 20 characters. *add* − Used to associate a profile to a multicast VLAN. *delete* − Used to de-associate a profile from a multicast VLAN. *ipv6_range <ipv6addr>* − Specified the IPv6 address range.
Restrictions	Only administrator, operator or power user–level users can issue this command.

Example usage:

To configure mld snooping multicast VLAN group mv2:

```
DGS-1210-28MP:5# config mld_snooping multicast_vlan_group mv2 add ipv6_range 3000::1 3000::3
Command: config mld_snooping multicast_vlan_group mv2 add ipv6_range 3000::1 3000::3

Success.
DGS-1210-28MP:5#
```

show mld_snooping multicast_vlan_group

Purpose	To display the multicast group profiles configured for the specified MLD multicast VLAN.
Syntax	**show mld_snooping multicast_vlan_group {<vlan_name 32>}**
Description	After binding a profile to a multicast VLAN, when a multicast group attempt to join this multicast VLAN member port, the group cannot join this multicast VLAN if the group does not belong to the range of binding profile.
Parameters	*<vlan_name 32>* − Specifies the name of multicast VLAN to be displayed.
Restrictions	None.

Example usage:

To display mld snooping multicast VLAN group:

```
DGS-1210-28MP:5# show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group

VID  Vlan Name                    IP Range
---- ------------------------------ ----------------------------------------

DGS-1210-28MP:5#
```

config mld_snooping mrouter_ports

Purpose	To enable mld mrouter ports.
Syntax	**config mld_snooping mrouter_ports** [vlan_name **<string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config mld_snooping mrouter_ports** command defines a port that is connected to a multicast router port.

Parameters	*vlan_name* <*string 32*> – specifies that the mld snooping applies only to this previously created VLAN. *vlanid* <*vidlist*> – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port. *delete* – Deletes a specified port to the mld snooping mrouter port. <*portlist*> – Defines the ports to be included from the mld snooping mrouter group.
Restrictions	Only administrator, operator or power user–level users can issue this command. Separate non–consecutive Ethernet ports with a comma and no spaces; use a hyphen to DGSignate a range of ports. These ports are defined as connected to a multicast router.

Example usage:

To configure mld mrouter ports:

```
DGS-1210-28MP:5# config mld_snooping mrouter_ports vlanid 1 add 1-3
Command: config mld_snooping mrouter_ports vlanid 1 add 1-3


Success.
DGS-1210-28MP:5#
```

config mld_snooping mrouter_ports_forbidden

Purpose	To define mld mrouter ports forbidden on the Switch.
Syntax	**config mld_snooping mrouter_ports_forbidden [vlan_name <string 32> | vlanid <vidlist> | all] [add | delete] <portlist>**
Description	The **config mld_snooping mrouter_ports_forbidden** command forbids a port from being defined as a multicast router port by static configuration or by automatic learning.
Parameters	*vlan_name* <*string 32*> – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid* <*vidlist*> – specifies that the mld snooping applies only to this previously created VLAN id. *all* – specifies that MLD snooping is to be configured for all VLANs on the Switch. *add* – Adds a specified port to the mld snooping mrouter port. *delete* – Deletes a specified port to the mld snooping mrouter port. <*portlist*> – Defines the ports to be included from the mld snooping mrouter group.
Restrictions	Only administrato–level users can issue this command.

Example usage:

To define the MLD snooping mrouter forbidden:

```
DGS-1210-28MP:5# config mld_snooping mrouter_ports_forbidden vlanid 1 add 8
Command: config mld_snooping mrouter_ports_forbidden vlanid 1 add 8
```

```
Success.
DGS-1210-28MP:5#
```

show mld_snooping mrouter_ports

Purpose	To display information on dynamically learnt and static multicast router interfaces.
Syntax	**show mld_snooping mrouter_ports [vlan <vlan_name 20> | vlanid <vidlist 1-4094> | all] [dynamic | static | forbidden]**
Description	The **show mld_snooping mrouter_ports** command displays on dynamically learnt and static multicast router interfaces.
Parameters	*vlan_name* <*string 32*> – Specifies on which VLAN mld snooping groups should be shown. *vlanid* <*vidlist*> – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch. *static* − Displays statically configured MLD router ports. *dynamic* − Displays dynamically configured MLD router ports. *forbidden* – Displays forbidden router ports that have been statically configured.
Restrictions	None.

Example usage:

To show the MLD_snooping mrouterport:

```
DGS-1210-28MP:5#  show mld_snooping router_ports vlanid 1
Command: show mld_snooping router_ports vlanid 1


VLAN  Name              : default
Static Router Port      : 3
Dynamic Router Port     :


Success.

DGS-1210-28MP:5#
```

show mld_snooping host

Purpose	To display information of MLD snooping host on the Switch.
Syntax	**show mld_snooping host [vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist> | group <ipv6_addr>]**
Description	The **show mld_snooping host** command displays information of MLD snooping host on the Switch.
Parameters	*vlan_name* <*string 32*> – Specifies on which VLAN mld snooping groups should be shown. *vlanid* <*vidlist*> – Displays that the mld snooping applies only to this previously created VLAN id.

	all – Displays that all MLD snooping which configured for all VLANs on the Switch. *ports <portlist>* – Specifies the ports of MLD snooping host to be displayed. *group <ipv6_addr>* – Specifies the IPv6 address.
Restrictions	None.

Example usage:

To show the MLD_snooping host:

```
DGS-1210-28MP:5#  show mld_snooping host vlan_name default
Command: show mld_snooping host vlan_name default



Total Entries : 0
DGS-1210-28MP:5#
```

show mld_snooping forwarding

Purpose	To display mld snooping settings on the Switch.
Syntax	**show mld_snooping forwarding [vlan_name <string 32> | vlanid <vidlist> | all]**
Description	The **show mld_snooping forwarding** command displays the current MLD snooping forwarding table entries currently configured on the Switch.
Parameters	*vlan_name <string 32>* – Displays that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – Displays that the mld snooping applies only to this previously created VLAN id. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch.
Restrictions	None.

Example usage:

To display the MLD snooping forwarding:

```
DGS-1210-28MP:5# show mld_snooping forwarding all
Command: show mld_snooping forwarding all



Total Entries : 0
DGS-1210-28MP:5#
```

show mld_snooping group

Purpose	To display mld snooping group settings on the Switch.
Syntax	**show mld_snooping group [vlan_name <string 32> | vlanid <vidlist> | all | ports <portlist>]**
Description	The **show mld_snooping group** command displays the multicast groups that were learned by MLD snooping.

Parameters	*vlan_name <string 32>* – The name of the VLAN for which to view the MLD snooping group configurations. *vlanid <vidlist>* – The id of the VLAN for which to view the MLD snooping group configurations. *all* – Displays that all MLD snooping which configured for all VLANs on the Switch. *ports <portlist>* – The ports of the VLAN for which to view the MLD snooping group configurations.
Restrictions	None.

Example usage:

To show the MLD snooping groups:

```
DGS-1210-28MP:5# show mld_snooping group all
Command: show mld_snooping group all


Total Entries : 0

DGS-1210-28MP:5#
```

config mld_snooping data_driven_learning

Purpose	To enable or disable the data-driven learning of an MLD snooping group on the Switch.
Syntax	**config mld_snooping data_driven_learning [max_learned_entry <value 1-1024>| vlan_name <string 32> | vlanid <vidlist> | all] [age_out [disable | enable] | expiry_time <sec 130-1530255> | state [enable | disable]]**
Description	The **config mld_snooping data driven_learning** command used to enable or disable the data-driven learning of an MLD snooping group.
Parameters	*max_learned_entry <value 1-1024>* – Speciifies the maximum learning entry value. *vlan_name <string 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *vlanid <vidlist>* – Specifies that the mld snooping applies only to this previously created VLAN id. *all* – Specifies that MLD snooping is to be configured for all VLANs on the Switch. *age_out [disable | disable]* –Enable or disable the aging out of entries. By default, the state is disabled. *expiry_time <sec 130-1530255>* –Specify the data driven group lifetime, in seconds. The value is between 130 and 1530255. *state [enable | disable]* –Specify to enable or disable the data driven learning of MLD snooping groups.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To enable the data driven learning of an MLD snooping group on the default VLAN:

```
ES-1210-28MP:5# config mld_snooping data_driven_learning vlan_name default state enable
```

```
Command: config mld_snooping data_driven_learning vlan_name default state
enable


Success !
DGS-1210-28MP:5#
```

config mld_snooping data_driven_learning

Purpose	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 dada-driven groups. Traffic for the new groups will be dropped.
Syntax	**config mld_snooping data_driven_learning max_learned_entry <integer 1-1024>**
Description	The **config mld_snooping data_driven_learning** command is used to configure the maximum number of groups that can be learned by data driven.
Parameters	*max_learned_entry <integer 1-1024>* – Specifies the maximum number of groups that can be learned by data drive. This value must be between 1 and 1024, and the suggested default setting is 56.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To set the maximum number of groups that can be learned by data driven:

```
DGS-1210-28MP:5# config mld_snooping data_driven_learning
max_learned_entry 50
Command: config mld_snooping data_driven_learning max_learned_entry 50


Success.
DGS-1210-28MP:5#
```

show mld_snooping statistics counter

Purpose	To display display the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.
Syntax	**show mld_snooping statistics counter [vlan_name <string 32> | vlanid <vlanid_list> | ports <portlist>]**
Description	The **show mld_snooping statistics counter** command displays the statistics counter for MLD protocol packets that are received by the Switch since MLD snooping was enabled.
Parameters	*vlan_name <string 32>* – Specifies on which VLAN name to be displayed. *vlanid <vidlist>* – Specifies on which VLAN ID to be displayed. *ports <portlist>* – Specifies the ports of MLD snooping ports to be displayed.
Restrictions	None.

Example usage:

To display the MLD_snooping statistics counter for port 1 to 3:

```
DGS-1210-28MP:5# show mld_snooping statistic counter ports 1-3
Command: show mld_snooping statistic counter ports 1-3

 Total Entries : 0


DGS-1210-28MP:5#
```

clear mld_snooping statistics counter

Purpose	To clear MLD snooping statistics counters.
Syntax	**clear mld_snooping statistics counter**
Description	The **clear mld_snooping statistics counter** command clears MLD snooping statistics counters.
Parameters	None.
Restrictions	Only administrator–level users can issue this command.

Example usage:

To clear the MLD_snooping statistics counters:

```
DGS-1210-28MP:5# clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter


Success.
DGS-1210-28MP:5#
```

24

LIMITED IP MULTICAST ADDRESS COMMANDS

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create mcast_filter_profile	[ipv4 | ipv6] profile_id <integer 1-24> profile_name string
config mcast_filter_profile	[profile_id <integer 1-24> | profile_name <string 32>] [add | delete] <mcast_addr>
config mcast_filter_profile ipv6	[profile_id <integer 1-24> | profile_name <string 32>] [add | delete] <ipv6_mcast_addr>
delete mcast_filter_profile	[ipv4 | ipv6] [profile_id<integer 1-24> | profile_name <string 32>]
show mcast_filter_profile	{[ipv4 | ipv6]} {profile_id <integer 1-24> | profile_name <string 32>}
config limited_multicast_addr	ports <portlist> [ipv4 | ipv6] {[add | delete] [profile_id <integer 1-24> | profile_name <string 20>] | access [permit | deny]}
show limited_multicast_addr	ports <portlist > {[ipv4 | ipv6]}
config max_mcast_group	ports <portlist> [ipv4 | ipv6] max_group <integer 1-32>
show max_mcast_group	ports <portlist > {[ipv4 | ipv6]}

Each command is listed in detail, as follows:

create mcast_filter_profile	
Purpose	To create multicast filtering profile on the Switch.
Syntax	**create mcast_filter_profile [ipv4 | ipv6] profile_id <integer 1-24> profile_name string**
Description	The **create mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be created on the Switch. *profile_id <integer 1-24>* - Specify the profile id of multicast filter profile on the Switch. *profile_name string* - Specify the profile name of multicast filter profile on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an IPv4 multicast filtering profile on the Switch:

```
DGS-1210-28MP:5# create mcast_filter_profile ipv4 profile_id 1 profile_name string
Command: create mcast_filter_profile ipv4 profile_id 1 profile_name string

Success.
DGS-1210-28MP:5#
```

config mcast_filter_profile

Purpose	To configure multicast filtering profile on the Switch.
Syntax	**config mcast_filter_profile [profile_id <integer 1-24> | profile_name <string 32>] [add | delete] <mcast_addr>**
Description	The **config mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*profile_id <integer 1-24>* - Specify the profile id to be added or deleted for the multicast filter. *profile_name <string 32>* - The name of the VLAN on which the MAC address resides. *[add | delete]* – Add or delete the profile id which user specified. <*mcast_addr*> – Specify the range of IPv4 address.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add the multicast address range 225.1.1.1 to 225.1.1.10 to the profile on the Switch:

```
DGS-1210-28MP:5# config mcast_filter_profile profile_id 3 add 225.1.1.1 225.1.1.10
Command: config mcast_filter_profile profile_id 3 add 225.1.1.1 225.1.1.10

Success.
DGS-1210-28MP:5#
```

config mcast_filter_profile ipv6

Purpose	To configure IPv6 multicast filtering profile on the Switch.
Syntax	**config mcast_filter_profile ipv6 [profile_id <integer 1-24> | profile_name <string 32>] [add | delete] <ipv6_mcast_addr>**
Description	The **config mcast_filter_profile ipv6** command is used to add or delete a range of IPv6 multicast addresses to the profile
Parameters	*profile_id <integer 1-24>* - Specify the profile id to be added or deleted for the multicast filter. *profile_name <string 32>* - The name of the VLAN on which the MAC address resides. *[add | delete]* – Add or delete the profile id which user specified. <*ipv6_mcast_addr*> – Lists the IPv6 multicast addresses to put in the profile
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add the IPv6 multicast address range FFF0E::100:0:0:20 – FFF0E::100:0:0:22 to profile ID 4 on the Switch:

```
DGS-1210-28MP:5# config mcast_filter_profile ipv6 profile_id 4 add
FF0E::100:0:0:20 FF0E::100:0:0:22
Command: config mcast_filter_profile ipv6 profile_id 4 add
FF0E::100:0:0:20 FF0E::100:0:0:22

Success.
DGS-1210-28MP:5#
```

delete mcast_filter_profile

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	**delete mcast_filter_profile [ipv4 | ipv6] [profile_id<integer 1-24> | profile_name <string 32>]**
Description	The **delete mcast_filter_profile** command deletes a profile in the Switch's multicast forwarding filtering database.
Parameters	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be removed on the Switch. *profile_id <integer 1-24>* − The profile id of the VLAN on which the multicast forwarding filtering database resides. *profile_name <string 32>* − The name of the VLAN on which the multicast forwarding filtering database resides.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete the IPv4 multicast address profile with a profile name of rd3:

```
DGS-1210-28MP:5# delete mcast_filter_profile ipv4 profile_name rd3
Command: delete mcast_filter_profile ipv4 profile_name rd3

Success.
DGS-1210-28MP:5#
```

show mcast_filter_profile

Purpose	To display multicast filtering settings on the Switch.
Syntax	**show mcast_filter_profile {[ipv4 | ipv6]} {profile_id <integer 1-24> | profile_name <string 32>}**
Description	The **show mcast_filter_profile** command displays the multicast filtering profiles settings.
Parameters	*[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be displayed on the Switch. *profile_id <integer 1-24>* - Specify the profile id of multicast filter profile to be displayed. *profile_name <string 32>* - Specify the profile name of multicast filter profile to be displayed.
Restrictions	None.

Example usage:

To display all the defined multicast address profiles:

```
DGS-1210-28MP:5#  show mcast_filter_profile ipv4 profile_id 1
Command: show mcast_filter_profile ipv4 profile_id 1

Mcast Filter Profile:

Profile ID      Name                        Multicast Addresses
--------------- ----------------------------  ----------------------------
1               string

Total Profile Count:   1

DGS-1210-28MP:5#
```

config limited_multicast_addr ports

Purpose	To configure the multicast address filtering function a port.
Syntax	**config limited_multicast_addr ports <portlist > [ipv4 | ipv6] {[add | delete] [max_group <integer 1-256> | access [permit | deny]}**
Description	The **config limited_multicast_addr ports** command is used to configure the multicast address filtering function on a port. When there are no profiles specified with a port, the limited function is not effective.
Parameters	*ports <portlist* > – A port or range of port on which the limited multicast address range to be configured has been assigned. *[ipv4* | *ipv6]* – Specify the IPv4 or IPv6 of multicast filter profile to be configured. *add* – Add a multicast address profile to a port. *delete* – Delete a multicast address profile to a port. *permit* – Specifies that the packet that matches the addresses defined in the profiles will be permitted. The default mode is permit. *deny* – Specifies that the packet matches the addresses defined in the profiles will be denied.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ports 1 and 3 to set the IPv6 multicast address profile id 1:

```
DGS-1210-28MP:5#  config limited_multicast_addr ports 1 ipv6 access permit
Command: config limited_multicast_addr ports 1 ipv6 access permit

Success.
DGS-1210-28MP:5#
```

show limited_multicast_addr ports

Purpose	Used to show the per-port Limited IP multicast address range.
Syntax	**show limited_multicast_addr ports <portlist > {[ipv4 | ipv6]}**
Description	The **show limited_multicast_addr ports** command is to display the

	multicast address range by port or by VLAN.
Parameters	*<portlist >* – Used to show the per-port Limited IP multicast address range. *[ipv4 | ipv6]* – Specify the IPv4 or IPv6 of limited multicast address to be displayed.
Restrictions	None.

Example usage:

To show the IPv4 limited multicast address on ports 1 and 3:

```
DGS-1210-28MP:5#  show limited_multicast_addr ports 1
Command: show limited_multicast_addr ports 1


Port  : 1
Access: permit

Profile ID     Name                        Multicast Addresses
-------------  --------------------------- ---------------------------


DGS-1210-28MP:5#
```

config max_mcast_group

Purpose	Used to configure the maximum number of multicast groups that a port can join.
Syntax	**config max_mcast_group ports <portlist> [ipv4 | ipv6] max_group <integer 1-32>**
Description	The **config max_mcast_group** command is used to configure the maximum number of multicast groups that a port can join.
Parameters	*<portlist>* – A range of ports to configure the maximum multicast group. *[ipv4 | ipv6]* – Specify the IPv4 or IPv6 to be configured. *max_group <integer 1-1024>* – Specifies the maximum number of multicast groups. The range is from 1 to 1024.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the IPv4 maximum multicast address groups on ports 1 and 3 as 100 with action drop:

```
DGS-1210-28MP:5# config max_mcast_group ports 1-3 ipv4 max_group 30
Command: config max_mcast_group ports 1-3 ipv4 max_group 30

Success.

DGS-1210-28MP:5#
```

show max_mcast_group ports	
Purpose	To display maximum multicast group ports on the Switch.
Syntax	**show max_mcast_group ports <portlist > {[ipv4 | ipv6]}**
Description	The **show max_mcast_group ports** command displays the multicast filtering profiles settings.
Parameters	*<portlist>* - Specify a port or range of ports to be displayed. *{[ipv4 | ipv6]}* – Specify the IPv4 or IPv6 to be displayed.
Restrictions	None.

Example usage:

To show IPv6 maximum multicast group port 1 settings:

```
DGS-1210-28MP:5# show max_mcast_group ports 1
Command: show max_mcast_group ports 1

Port        IPv4 MaxMcastGroup      IPv6 MaxMcastGroup
-----       --------------------    --------------------
1           30                      32

DGS-1210-28MP:5#
```

25

802.1X COMMANDS

The 802.1X commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable 802.1x	
disable 802.1x	
show 802.1x	
show 802.1x auth_state	{ports <portlist >}
show 802.1x auth_configuration	{ports <portlist >}
config 802.1x auth_parameter ports	[<portlist > | all] [default | { 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> | enable_reauth [enable | disable] | direction [both | in]}]
config 802.1x auth_protocol	[radius_eap | local]
config radius add	<server_index 1-3> [<ipaddr> | <ipv6addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <int 1-255> | retransmit <int 1-255>}
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> { key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | ipaddress [<ipaddr> | <ipv6addr>] | retransmit <int 1-255> | timeout <int 1-255>}
show radius	
config 802.1x auth_mode	[port_based | mac_based]
create 802.1x guest_vlan	<vlan_name 20>
delete 802.1x guest_vlan	<vlan_name 20>
config 802.1x guest_vlan ports	[<portlist > | all] state [enable | disable]
show 802.1x guest_vlan	
create 802.1x user	<username 15>
config 802.1x user	<username 15> Password <value 15>
show 802.1x user	

Command	Parameter
delete 802.1x user	<username 15>
config 802.1x capability ports	[<portlist > | all] [authenticator | none]
config 802.1x init	port_based ports [<portlist> | all]
config 802.1x reauth	port_based ports [<portlist> | all]
config 802.1x fwd_pdu system	[enable | disable]
show 802.1x fwd_pdu system status	

Each command is listed in detail, as follows:

enable 802.1x	
Purpose	To enable the 802.1x server on the Switch.
Syntax	**enable 802.1x**
Description	The **enable 802.1x** command enables the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable 802.1x:

```
DGS-1210-28MP:5# enable 802.1x
Command: enable 802.1x

Success.
DGS-1210-28MP:5#
```

disable 802.1x	
Purpose	To disable the 802.1x server on the Switch.
Syntax	**disable 802.1x**
Description	The **disable 802.1x** command disables the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable 802.1x:

```
DGS-1210-28MP:5# disable 802.1x
Command: disable 802.1x

Success.
```

```
DGS-1210-28MP:5#
```

show 802.1x

Purpose	To display the 802.1x server information on the Switch.
Syntax	**show 802.1x**
Description	The **show 802.1x** command displays the 802.1x Port-based Network Access control server application on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display 802.1x parameters:

```
DGS-1210-28MP:5# show 802.1x
Command: show 802.1x

802.1X                    : Enable
Authentication Mode       : Port_base
Authentication Method     : Local
DGS-1210-28MP:5#
```

show 802.1x auth_state

Purpose	To display the current authentication state of the 802.1x server on the Switch.
Syntax	**show 802.1x auth_state {ports <portlist >}**
Description	The **show 802.1x auth_state** command displays the current 802.1x authentication state of the specified ports of the Port-based Network Access Control server application on the Switch. The following details are displayed: Port number − Shows the physical port number on the Switch. Auth PAE State: Initialize / Disconnected / Connecting / Authenticating / Authenticated / Held / ForceAuth / ForceUnauth − Shows the current state of the Authenticator PAE. Backend State: Request / Response / Fail / Idle / Initialize / Success / Timeout − Shows the current state of the Backend Authenticator. Port Status: Authorized / Unauthorized − Shows the result of the authentication process. Authorized means that the user was authenticated, and can access the network. Unauthorized means that the user was not authenticated, and cannot access the network.
Parameters	*ports <portlist* > − A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the 802.1x authentication states:

```
DGS-1210-28MP:5# show 802.1x auth_state ports 1-3
Command: show 802.1x auth_state ports 1-3
```

```
Port   Auth PAE State  Backend State   Port Status
------ -------------- -------------   ------------
1      ForceAuth      Success         Authorized
2      ForceAuth      Success         Authorized
3      ForceAuth      Success         Authorized
DGS-1210-28MP:5#
```

show 802.1x auth_configuration

Purpose	To display the current configuration of the 802.1x server on the Switch.
Syntax	**show 802.1x auth_configuration {ports <portlist >}**
Description	The **show 802.1x auth_configuration** command displays the current configuration of the 802.1x Port-based Network Access Control server application on the Switch. The following details are displayed: *802.1x:* Enabled/Disabled − Shows the current status of 802.1x functions on the Switch. *Authentication Mode:* Port-based/Mac-based/None − Shows the 802.1x authorization mode. Authentication Method: Remote/none − Shows the type of authentication protocol suite in use between the Switch and a RADIUS server. *Port number :* Shows the physical port number on the Switch. *AdminCrlDir:* Both/In − Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. *OpenCrlDir:* Both/In − Shows whether a controlled Port that is unauthorized will exert control over communication in both receiving and transmitting directions, or just the receiving direction. *Port Control:* ForceAuth/ForceUnauth/Auto − Shows the administrative control over the port's authorization status. ForceAuth forces the Authenticator of the port to become Authorized. ForceUnauth forces the port to become Unauthorized. *QuietPeriod :* Shows the time interval between authentication failure and the start of a new authentication attempt. *TxPeriod :* Shows the time to wait for a response from a supplicant (user) to send EAP Request/Identity packets. *SuppTimeout :* Shows the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. *ServerTimeout :* Shows the length of time to wait for a response from a RADIUS server. *MaxReq :* Shows the maximum number of times to retry sending packets to the supplicant. *ReAuthPeriod :* Shows the time interval between successive reauthentications. *ReAuthenticate:* true/false − Shows whether or not to reauthenticate.
Parameters	*ports <portlist >* − Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display the 802.1x configurations of port 2:

```
DGS-1210-28MP:5#  show 802.1x auth_configuration ports 2
Command: show 802.1x auth_configuration ports 2

Port number      : 2
Capability       : none
AdminCrlDir      : Both
OperCrlDir       : Both
Port Control     : ForceAuthorized
QuietPeriod      : 60    sec
TxPeriod         : 30    sec
SuppTimeout      : 30    sec
ServerTimeout    : 30    sec
MaxReq           : 2     times
ReAuthPeriod     : 3600  sec
ReAuthenticate   : Disabled

Success.
DGS-1210-28MP:5#
```

config 802.1x auth_parameter ports

Purpose	To configure the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.
Syntax	**config 802.1x auth_parameter ports [<portlist > | all] [default | { 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 > | reauth_period <sec 1-65535> | enable_reauth [enable | disable] | direction [both | in]}]**
Description	The **config 802.1x auth_parameter ports** command configures the 802.1x authentication parameters on a range of ports. The default parameter returns all ports in the specified range to their default 802.1x settings.
Parameters	*[<portlist* > | *all]* – A port, range of ports or all ports to be configured. *all* – Specifies all of the ports on the Switch. *default* – Returns all of the ports in the specified range to their 802.1x default settings. *port_control* – Configures the administrative control over the authentication process for the range of ports. The options are: • *force_auth* – Forces the Authenticator for the port to become authorized. Network access is allowed. • *auto* – Allows the port's status to reflect the outcome of the authentication process. • *force_unauth* – Forces the Authenticator for the port to become unauthorized. Network access is blocked. *quiet_period <sec 0-65535>* – Configures the time interval between authentication failure and the start of a new authentication attempt. *tx_period <sec 1-65535>* - Configures the time to wait for a

	response from a supplicant (user) to send EAP Request/Identity packets. *supp_timeout* <*sec 1-65535*> - Configures the time to wait for a response from a supplicant (user) for all EAP packets, except for the Request/Identity packets. *server_timeout* <*sec 1-65535*> - Configures the length of time to wait for a response from a RADIUS server. *max_req* <*value* > – Configures the number of times to retry sending packets to a supplicant (user). *reauth_period* <*sec 300-4294967295*> – Configures the time interval between successive re-authentications. *enable_reauth [enable*	*disable]* – Determines whether or not the Switch will re-authenticate. Enabled causes re-authentication of users at the time interval specified in the Re-authentication Period field, above. *direction [both*	*in]* –Sets the administrative-controlled direction to *Both*. If *Both* is selected, control is exerted over both incoming and outgoing traffic through the controlled port selected in the first field. The *In* option is not supported in the present firmware release.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure 802.1x authentication parameters:

```
DGS-1210-28MP:5# config 802.1x auth_parameter ports 1-3 direction both
Command: config 802.1x auth_parameter ports 1-3 direction both

Success.
DGS-1210-28MP:5#
```

config 802.1x auth_protocol

Purpose	To configure the 802.1x authentication protocol on the Switch .
Syntax	**config 802.1x auth_protocol [radius_eap | local]**
Description	The **config 802.1x auth_protocol** command enables configuration of the authentication protocol.
Parameters	*radius_eap* – Uses the list of RADIUS EAP servers for authentication. *local* – Uses no authentication.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS (AAA) authentication protocol on the Switch:

```
DGS-1210-28MP:5# config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success.
DGS-1210-28MP:5#
```

config radius add

Purpose	To configure the settings the Switch uses to communicate with a RADIUS server.
Syntax	**config radius add <server_index 1-3> [<ipaddr> | <ipv6addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout <int 1-255> | retransmit <int 1-255>}**
Description	The **config radius add** command configures the settings the Switch uses to communicate with a RADIUS server.
Parameters	*<server_index 1-3>* – The index of the RADIUS server. *[<ipaddr>* | *<ipv6_addr]>* – The IPv4 or IPv6 address of the RADIUS server. *key* – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server. *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used. *default* – Uses the default udp port number in both the *auth_port* and *acct_port* settings. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813. *retransmit <int 1-255>* –The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. *timeout <int 1-255>* –Specifies the connection timeout. The value may be between 1 and 255 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS server:

```
DGS-1210-28MP:5#  config radius add 1 10.90.90.99 key dfjk auth_port 100 acct_port 1000 timeout 1 retransmit 10
Command: config radius add 1 10.90.90.99 key dfjk auth_port 100 acct_port 1000 timeout 1 retransmit 10


Success.
DGS-1210-28MP:5#
```

config radius delete

Purpose	To delete a previously entered RADIUS server configuration.
Syntax	**config radius delete <server_index 1-3>**
Description	The **config radius delete** command deletes a previously entered RADIUS server configuration.
Parameters	*<server_index 1-3>* – The index of the RADIUS server.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server:

```
DGS-1210-28MP:5# config radius delete 1
Command: config radius delete 1

Success.
DGS-1210-28MP:5# #
```

config radius

Purpose	To configure the Switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> { key <passwd 32> | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | ipaddress [<ipaddr> | <ipv6addr>] | retransmit <int 1-255> | timeout <int 1-255>}**
Description	The **config radius** command configures the Switch's RADIUS settings.
Parameters	*<server_index 1-3>* – The index of the RADIUS server. *key* – Specifies that a password and encryption key are to be used between the Switch and the RADIUS server. • *<passwd 32>* – The shared-secret key used by the RADIUS server and the Switch. Up to 128 characters can be used. *auth_port <udp_port_number 1-65535>* – The UDP port number for authentication requests. The default is 1812. *acct_port <udp_port_number 1-65535>* – The UDP port number for accounting requests. The default is 1813. *ipaddress [<ipaddr> | <ipv6addr>]* – The IPv4 or IPv6 address of the RADIUS server. *retransmit <int 1-255>* –The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255. *timeout <int 1-255>* –Specifies the connection timeout. The value may be between 1 and 255 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-1210-28MP:5# config radius 1 ipaddress 10.48.47.11
Command: config radius 1 ipaddress 10.48.47.11

Success.
DGS-1210-28MP:5#
```

show radius

Purpose	To display the current RADIUS configurations on the Switch.
Syntax	**show radius**
Description	The **show radius** command displays the current RADIUS configurations on the Switch.

Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS settings:

```
DGS-1210-28MP:5# show radius
Command: show radius

Index  Ip Address      Auth-Port  Acct-Port  Timeout  Retransmit  Key
-----  ----------------  ---------  ----------  ---------  ---------------  ------
1      10.48.74.121    1812       1813       5        10          dlink

Total Entries : 1
DGS-1210-28MP:5#
```

config 802.1x auth_mode

Purpose	To configure the 802.1x authentication mode on the Switch.
Syntax	**config 802.1x auth_mode [port_based | mac_based]**
Description	The **config 802.1x auth_mode** command enables either the port-based or MAC-based 802.1x authentication feature on the Switch.
Parameters	*[port_based* | *mac_based]* – Specifies whether 802.1x authentication is by port or MAC address.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure 802.1x authentication by port address:

```
DGS-1210-28MP:5# config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.
DGS-1210-28MP:5#
```

create 802.1x guest_vlan

Purpose	Enables network access to a Guest VLAN.
Syntax	**create 802.1x guest vlan <vlan_name 20>**
Description	The **create 802.1x guest_vlan** command enables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	*<vlan_name 20>* − The name of the 802.1x Guest VLAN to be created.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a 802.1x Guest VLAN:

```
DGS-1210-28MP:5# create 802.1x guest_vlan default
Command: create 802.1x guest_vlan default

Success.
DGS-1210-28MP:5#
```

delete 802.1x guest_vlan

Purpose	Disables network access to a Guest VLAN.
Syntax	**delete 802.1x guest vlan <vlan_name 20>**
Description	The **delete 802.1x guest_vlan** command disables network access to a 802.1x Guest VLAN. A network administrator can use 802.1x Guest VLANs to deny network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	*<vlan_name 20>* − The name of the 802.1x Guest VLAN to be deleted.
Restrictions	Only Administrator or operator-level users can issue this command. The user is required to disable Guest VLAN before deleting a specific the VLAN.

Example usage:

To delete specified 802.1x Guest VLAN

```
DGS-1210-28MP:5# delete 802.1x guest_vlan default
Command: delete 802.1x guest_vlan default

Success.
DGS-1210-28MP:5#
```

config 802.1x guest_vlan ports

Purpose	Defines a port or range of ports to be members of the Guest VLAN.
Syntax	**config 802.1x guest_vlan ports [<portlist > | all] state [enable | disable]**
Description	The **config 802.1x guest_vlan ports** command defines a port or range of ports to be members of the 802.1x Guest VLAN. The 802.1x Guest VLAN can be be configured to provide limited network access to authorized member ports. If a member port is denied network access via port–based authorization, but the 802.1x Guest VLAN is enabled, the member port receives limited network access. For example, a network administrator can use the 802.1x Guest VLAN to deny internal network access via port–based authentication, but grant Internet access to unauthorized users.
Parameters	*<portlist >* – A port or range of ports to be configured to the Guest VLAN. *all* – Indicates all ports to be configured to the guest vlan. *state [enable | disable]* – Specifies the guest vlan port is enabled or disabled of the switch.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure ports to the Guest VLAN:

```
DGS-1210-28MP:5# config 802.1x guest_vlan ports 1-3 state enable
Command: config 802.1x guest_vlan ports 1-3 state enable

Success.
DGS-1210-28MP:5#
```

show 802.1x guest_vlan

Purpose	Displays configuration information for the Guest VLAN.
Syntax	**show 802.1x guest_vlan**
Description	The **show 802.1x guest_vlan** command displays the Guest VLAN name, state, and member ports.
Parameters	None.
Restrictions	None.

Example usage:

To display the Guest VLAN configuration:

```
DGS-1210-28MP:5# show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Settings
------------------------------------------------------------------------
Guest VLAN                  : default
Enabled Guest VLAN Ports    : 1,2,3,4,5,6

DGS-1210-28MP:5#
```

create 802.1x user

Purpose	Create user account for local database for 802.1x.
Syntax	**create 802.1x user <username 15>**
Description	The **create 802.1x user** command enables network access to a 802.1x user.
Parameters	<*vlan_name 15*> − The name of the 802.1x user to be created.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a 802.1x user:

```
DGS-1210-28MP:5#  create 802.1x user dlink
Command: create 802.1x user dlink

Enter a case-sensitive new password:****
Enter the new password again for confirmation:****
Success.
DGS-1210-28MP:5#
```

config 802.1x user

Purpose	Configure user account for local database for 802.1x.
Syntax	**config 802.1x user <username 15> password <value 15>**
Description	The **config 802.1x user** command is used to configure the user account password.
Parameters	*user <username 15>* − Specify the user account. *password <value 15>* − Specify the password string.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure 802.1x user:

```
DGS-1210-28MP:5# config 802.1x user dlink Password
2345
Command: config 802.1x user dlink Password ******


Success.

DGS-1210-28MP:5#
```

show 802.1x user

Purpose	Displays the user information for the 802.1x.
Syntax	**show 802.1x user**
Description	The **show 802.1x user** command displays the 802.1x user information on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the 802.1x user information:

```
DGS-1210-28MP:5# show 802.1x user
Command: show 802.1x user

Index       Username
----------  ---------------
 1          dlink

Total Entries: 1
Success.
DGS-1210-28MP:5#
```

delete 802.1x user

Purpose	Deletes network access to a 802.1x user.
Syntax	**delete 802.1x user <username 15>**
Description	The **delete 802.1x user** command deletes network access to a 802.1x user.
Parameters	<*vlanname 15*> − The name of the 802.1x user to be deleted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete the 802.1x user:

```
DGS-1210-28MP:5# delete 802.1x user dlink
Command: delete 802.1x user dlink


Success.
DGS-1210-28MP:5#
```

config 802.1x capability ports

Purpose	Defines a port or range of ports to be members of the 802.1x.
Syntax	**config 802.1x capability ports [<portlist > | all] [authenticator | none]**
Description	Th **config 802.1x capability ports** is used to configure the capability for the 802.1x on the Switch.
Parameters	<*portlist* > – A port or range of ports to be configured to the 802.1x capability. *all* – Indicates all ports to be configured to the 802.1x capability. *[authenticator* | *none]* – Specifies the 802.1x capability port to be authenticator or none.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure capability ports to the 802.1x:

```
DGS-1210-28MP:5# config 802.1x capability ports all authenticator
Command: config 802.1x capability ports all authenticator

Success.
DGS-1210-28MP:5#
```

config 802.1x init

Purpose	To initialize the 802.1x function on a range of ports.
Syntax	**config 802.1x init port_based ports [<portlist> | all]**
Description	The **config 802.1x init** command initializes the 802.1x functions on a specified range of ports or for specified MAC addresses operating from a specified range of ports.
Parameters	*port_based* – Instructs the Switch to initialize 802.1x functions based only on the port number. Ports approved for initialization can then be specified. *ports* <*portlist*> – A port or range of ports to be configured. *all* – Specifies all of the ports on the Switch.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To initialize the authentication state machine of all ports:

```
DGS-1210-28MP:5# config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.
DGS-1210-28MP:5#
```

config 802.1x reauth

Purpose	To configure the 802.1x re-authentication feature of the Switch.
Syntax	**config 802.1x reauth port_based ports [<portlist> | all]**
Description	The **config 802.1x reauth** command re-authenticates a previously authenticated device based on port number.
Parameters	*port_based* – Instructs the Switch to re-authorize 802.1x functions based only on the port number. Ports approved for re-authorization can then be specified. *ports* <*portlist*> – A port or range of ports to be re-authorized. *all* – Specifies all of the ports on the Switch.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-18:

```
DGS-1210-28MP:5# config 802.1x reauth port_based ports 1-18
Command: config 802.1x reauth port_based ports 1-18

Success.
DGS-1210-28MP:5#
```

config 802.1x fwd_pdu system

Purpose	To configure the 802.1x forwarding EAPOL PDU on the Switch.
Syntax	**config 802.1x fwd_pdu system [enable | disable]**
Description	The **config 802.1x fwd_pdu system** command is used to configure the control of forwarding EAPOL PDUs. Then the 802.1x functionality is disabled, for a port, and if the 802.1x forwarding PDU is enabled both globally and for the port, a received EAPOL packet on the port will be flooded on the same VLAN to those ports of which the 802.1x forwarding PDU is enabled and 802.1x is disabled (globally or just for the port).
Parameters	*[enable* | *disable]* – Specifies the forwarding of EAPOL PDU is enabled or disabled. The default is disabled.
Restrictions	Only Administrator, operator or power user-level users can issue this command.

Example usage:

To enable 802.1x forwarding EAPOL PDU

```
DGS-1210-28MP:5# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable


Success.
DGS-1210-28MP:5#
```

show 802.1x fwd_pdu system status

Purpose	To display the 802.1x forwarding EAPOL PDU status on the Switch.
Syntax	**show 802.1x fwd_pdu system status**
Description	The **show 802.1x fwd_pdu system status** command is used to display the control of forwarding EAPOL PDUs.
Parameters	None.
Restrictions	None.

Example usage:

To show 802.1x forwarding EAPOL PDU status:

```
DGS-1210-28MP:5# show 802.1x fwd_pdu system status
Command: show 802.1x fwd_pdu system status

PNAC control packet (eap) is forwarding....

Success.
DGS-1210-28MP:5#
```

26

PORT SECURITY COMMANDS

The Port Security commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config port_security	[<portlist> | all] [admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]
show port_security	{ports <portlist>}
delete port_security_entry	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>
clear port_security_entry	[all | port <portlist>]

Each command is listed in detail, as follows:

config port_security

Purpose	To configure port security settings.
Syntax	**config port_security [<portlist > | all] [admin_state [enable | disable] | max_learning_addr <max_lock_no 0-64> | lock_address_mode [Permanent | DeleteOnTimeout | DeleteOnReset]**
Description	The **config port_security** command configures port security settings for specific ports.
Parameters	*<portlist >* – A port or range of ports to be configured. *all* – Configures port security for all ports on the Switch. *admin_state [enable* | *disable]* – Enables or disables port security for the listed ports. *max_learning_addr <int 0-64>* - Specify the max learning address. The range is 0 to 64. 1-64 Limits the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode – Defines the TBD and contains the following options:* • *Permenant – Learns up to the maximum number of dynamic addresses allowed on the port. The learned addresses are not aged out or relearned on other port for as long as the port is locked.* • *DeleteOnReset – Deletes the current dynamic MAC addresses associated with the port. Learn up to the maximum addresses allowed on the port (this number is also configurable). Aging is disabled; the addresses are deleted on reset* • *DeleteOnTimeout – Deletes the current dynamic MAC addresses associated with the port. The port learns up to*

	the maximum addresses allowed on the port. Re-learned MAC addresses and address aging out are also enabled. The MAC addresses are deleted when the device is reset and on when the address is aged out.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To configure port security:

```
DGS-1210-28MP:5# config port_security 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset
Command: config port_security 1-5 admin_state enable
max_learning_addr 5 lock_address_mode DeleteOnReset


Success.

DGS-1210-28MP:5#
```

show port_security

Purpose	To display the current port security configuration.
Syntax	**show port_security {ports <portlist >}**
Description	The **show port_security** command displays port security information for the Switch's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode and trap interval.
Parameters	*ports <portlist >* – A port or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-1210-28MP:5# show port_security ports 1-5
Command: show port_security ports 1-5


Port  Admin state Max.Learning Addr. Lock Address Mode
----  ----------- -------------------------- -------------------
1     enabled     5                          DeleteOnReset
2     enabled     5                          DeleteOnReset
3     enabled     5                          DeleteOnReset
4     enabled     5                          DeleteOnReset
5     enabled     5                          DeleteOnReset

DGS-1210-28MP:5#
```

delete port_security _entry	
Purpose	To delete a port security entry by VLAN, VLAN ID, and MAC address.
Syntax	**delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>**
Description	The **delete port_security_entry** command is used to delete a port security entry by VLAN, VLAN ID, and MAC address.
Parameters	*<vlan_name 32>* – Specifies the VLAN name. *<vlanid 1-4094>* - Specifies the VLAN ID. *<macaddr>* - Specifies the MAC address.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the port security entry with a MAC address of 00-01-30-10-2c-c7 on the default VLAN:

```
DGS-1210-28MP:5# delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7

Command: delete port_security_entry vlan default mac_address 00-01-30-10-2C-C7


Success.

DGS-1210-28MP:5#
```

clear port_security _entry	
Purpose	To clear the MAC entries learned by the port security function.
Syntax	**clear port_security_entry [all | port <portlist>]**
Description	The **clear port_security_entry** command is used to clear the MAC entries learned by the port security function.
Parameters	*[all | port <portlist>]* – Specify all ports or a list of port for MAC entries to be cleared.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To clear all port security entries:

```
DGS-1210-28MP:5# clear port_security_entry all

Command: clear port_security_entry all



Success.


DGS-1210-28MP:5#
```

27

SPANNING TREE COMMANDS

The Spanning Tree commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config stp	{maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> | maxhops <value 6-40>}
config stp ports	<portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | hellotime <value 1-2> | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable] | migrate [yes | no] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }
config stp version	[mstp | rstp | stp]
config stp fbpdu	[enable | disable]
config stp priority	<value 0-61440> instance_id <value 0-63>
enable stp	
disable stp	
show stp	
show stp ports	{<portlist>}
show stp instance	{<value 1-63>}
show stp mst_config_id	
create stp instance_id	<value 1-63>
delete stp instance_id	<value 1-63>
config stp instance_id	<value 1-63> [add_vlan | remove_vlan] <vidlist>
config stp mst_config_id	[revision_level <int 0-65535> | name <string 32>]
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]}

Each command is listed in detail, as follows:

config stp	
Purpose	To setup STP, RSTP and MSTP on the Switch.
Syntax	**config stp {maxage <value 6-40> | hellotime <value 1-10> | forwarddelay <value 4-30>| txholdcount <value 1-10> | maxhops <value 6-40>}**
Description	The **config stp** command configures the Spanning Tree Protocol (STP) for the entire switch. All commands here are implemented for the STP version that is currently set on the Switch.

Parameters	*maxage* <*value 6-40*> − This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value aids in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch starts sending its own BPDU to all other switches for permission to become the Root Bridge. If your switch has the lowest priority, it becomes the Root Bridge. The user may choose a time between 6 and 40 seconds. The default value is 20. *hellotime* <*value 1-10*> − The user may set the time interval between transmission of configuration messages by the root device in STP, or by the DGSignated router, thus stating that the Switch is still functioning. The value may be between 1 and 10 seconds. The default value is 2 seconds. *forwarddelay* <*value 4-30*> − The amount of time (in seconds) that the root device will wait before changing from Blocking to Listening , and from Listening to Learning states. The value may be between 4 and 30 seconds. The default is 15 seconds. *txholdcount* <*value 1-10*> − The maximum number of BPDU Hello packets transmitted per interval. Default value = 3. *maxhops* <*value 6-40*> - The maximum number of BPDU hops packets transmitted per interval. Default value = 20.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and hellotime 2:

```
DGS-1210-28MP:5# config stp maxage 18 hellotime 2
Command: config stp maxage 18 hellotime 2

Success.
DGS-1210-28MP:5#
```

config stp ports

Purpose	To setup STP on the port level.
Syntax	**config stp ports <portlist> {externalcost [auto | <value 1-200000000>] | edge [auto | true | false] | hellotime <value 1-2> | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable | disable] | migrate [yes | no] | priority <value 0-240> | restricted_role [true | false] | restricted_tcn [true | false] }**
Description	The **config stp ports** command configures STP for a group of ports.
Parameters	<*portlist*> – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *externalCost* − Defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is auto. • *auto* – Automatically sets the speed for forwarding packets to the specified port(s) in the list for optimal efficiency.

	Default port cost:10Mbps port = 2000000. 100Mbps port = 200000. Gigabit port = 20000. Port-channel = 20000. • <*value 1-200000000*> - Defines a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *edge [auto* | *true* | *false]* – *true* DGSignates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. The default setting for this parameter is false. *hellotime* <*value 1-2*> – The time interval between transmission of configuration messages by the DGSignated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and 2 seconds. The default is 2 seconds. *p2p [true* | *false* | *auto]* – *true* indicates a point-to-point (P2P) link. P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of *false* indicates that the port cannot have p2p status. *auto* allows the port to have p2p status whenever possible and operate as if the p2p status were true. (A port that operates in full-duplex is assumed to be point-to-point, while a half-duplex port is considered as a shared port). If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *false*. The default setting for this parameter is *auto*. *state [enable* | *disable]* − Allows STP to be enabled or disabled for the ports specified in the port list. The default is enabled. *fbpdu [enable* | *disable* | *system]* − If enabled - allows the forwarding of STP BPDU packets from other network devices Disable – blocking STP BPDU packets from other network devices. System – indicates that port will behave as global switch's fbpdu value configured. Fbpdu value valid only when STP port state is disabled or global STP state is disabled. The default is system. *migrate [yes* | *no]* − Setting this parameter as "yes" will set the ports to send out BPDU packets to other bridges, requesting information on their STP setting if the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP to 802.1w RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1D STP to 802.1s MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where and 802.1D network connects to and 802.1w or 802.1s enabled network. Migration should be set as yes on ports connected to network stations or segments that are capable of being upgraded to 802.1w RSTP or 802.1s MSTP on all or some portion of the segment. *priority* <*value 0-240*> − Specifies the priority. The range is from 0 to 240. *restricted_role [true* | *false]* − To decide if this is to be selected as the Root Port. The default value is false. *restricted_tcn [true* | *false]* − To decide if this port is to propagate topology change. The default value is false.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure STP with path cost 19 and state enable for ports 1-3:

```
DGS-1210-28MP:5# config stp ports 1-3 externalcost 19 state enable
Command: config stp ports 1-3 externalcost 19 state enable

Success.
DGS-1210-28MP:5#
```

config stp version

Purpose	To globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	The **config stp version** command sets the version of the spanning tree to be implemented on the Switch.
Parameters	*mstp* – Sets the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Sets the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Sets the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the Switch globally for the Multiple Spanning Tree Protocol (MSTP):

```
DGS-1210-28MP:5# config stp version mstp
Command: config stp version mstp

Success.
DGS-1210-28MP:5#
```

config stp fbpdu

Purpose	To globally set the fbpdu of STP on the Switch.
Syntax	**config stp fbpdu [enable | disable]**
Description	The **config stp fbpdu** command allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the Switch globally for the Spanning Tree Protocol (STP) fbpdu enable:

```
DGS-1210-28MP:5# config stp fbpdu enable
Command: config stp fbpdu enable

Success.
DGS-1210-28MP:5#
```

config stp priority

Purpose	To update the STP instance configuration.
Syntax	**config stp priority <value 0-61440> instance_id <value 0-15>**
Description	The **config stp priority** command updates the STP instance configuration settings on the Switch. The MSTP uses the priority in selecting the root bridge, root port and DGSignated port. Assigning higher priorities to STP regions instructs the Switch to give precedence to the selected instance_id for forwarding packets. A lower value indicates a higher priority.
Parameters	*priority <value 0-61440>* - The priority for a specified *instance_id* for forwarding packets. The value may be between 0 and 61440, and must be divisible by 4096. A lower value indicates a higher priority. *instance_id <value 0-15>* - The value of the previously configured instance id for which the user wishes to set the priority value. An instance_id of 0 denotes the default instance_id (CIST) internally set on the Switch.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To set the priority value for instance_id 2 as 4096:

```
DGS-1210-28MP:5# config stp priority 4096 instance_id 2
Command: config stp priority 4096 instance_id 2

Success.
DGS-1210-28MP:5#
```

enable stp

Purpose	To globally enable STP on the Switch.
Syntax	**enable stp**
Description	The **enable stp** command is used to set the Spanning Tree Protocol to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DGS-1210-28MP:5# enable stp
Command: enable stp

Success.
DGS-1210-28MP:5#
```

disable stp

Purpose	To globally disable STP on the Switch.
Syntax	**disable stp**
Description	The **disable stp** command is used to set the Spanning Tree

	Protocol to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DGS-1210-28MP:5# disable stp
Command: disable stp

Success.
DGS-1210-28MP:5#
```

show stp

Purpose	To display the Switch's current STP configuration.
Syntax	**show stp**
Description	The **show stp** command displays the Switch's current STP configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

Status 1: STP enabled with STP compatible version

```
DGS-1210-28MP:5# show stp
Command: show stp


STP Bridge Global Settings
-----------------------------------------------
STP Status              : Enabled
STP Version             : RSTP
Bridge Priority         : 32768
Max Age                 : 18
Hello Time              : 2
Forward Delay           : 15
TX Hold Count           : 6
Forward BPDU            : Enabled
Root Cost               : 0
Root Maximum Age        : 18
Root Forward Delay      : 15
Root Port               : 0
Root Bridge             : 80:00:9C:D6:43:60:4F:A4

DGS-1210-28MP:5#
```

Status 2: STP enabled for RSTP

```
DGS-1210-28MP:5# show stp
Command: show stp

STP Bridge Global Settings
-----------------------------------------------------
STP Status                : Enabled
STP Version               : RSTP
Bridge Priority           : 32768
Max Age                   : 8
Hello Time                : 2
Forward Delay             : 15
TX Hold Count             : 6
Forward BPDU              : Enabled
Root Cost                 : 0
Root Maximum Age          : 8
Root Forward Delay        : 15
Root Port                 : 0
Root Bridge               : 80:00:9C:D6:43:60:4F:A4

DGS-1210-28MP:5#
```

Status 3: STP enabled for MSTP

```
DGS-1210-28MP:5# show stp
Command: show stp

STP Bridge Global Settings
------------------------------
STP Status                : Enabled
STP Version               : MSTP
Bridge Priority           : 32768
Max Age                   : 8
Hello Time                : 2
Forward Delay             : 15
TX Hold Count             : 6
Forward BPDU              : Enabled
Root Cost                 : 0
Root Maximum Age          : 8
Root Forward Delay        : 15
Root Port                 : 0
Root Bridge               : 80:00:9C:D6:43:60:4F:A4

DGS-1210-28MP:5#
```

show stp ports

Purpose	To display the Switch's current instance_id configuration.
Syntax	**show stp ports {<portlist>}**

Description	The **show stp ports** command displays the STP Instance Settings and STP Instance Operational Status currently implemented on the Switch.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To show stp port 1 on switch one:

```
DGS-1210-28MP:5# show stp ports 1
Command: show stp ports 1

MSTP      Port Information
-----------------------------------------------------------------
Port Index:1 ,  Port STP:Enabled ,      P2P:Auto ,
External PathCost : 19 ,       Edge Port:Auto ,
Port RestrictedRole:False ,     Port RestrictedTCN:False
Port Priority:128 ,     Port Forward BPDU:Enabled ,
MSTI DGSignated Bridge              Internal PathCost  Prio  Status     Role
-------  -------------------------          ----------------------     ----    ----------   ----------
0        80:00:00:B2:FD:DA:EE:EB  200000              128   Disabled  Disabled

DGS-1210-28MP:5#
```

show stp instance

Purpose	To display the Switch's STP instance configuration
Syntax	**show stp instance {<value 1-63>}**
Description	The **show stp instance** command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	*<value 1-63>* - The value of the previously configured instance_id on the Switch. The value may be between 1 and 63.
Restrictions	None.

Example usage:

To display the STP instance configuration on the Switch:

```
DGS-1210-28MP:5# show stp instance
Command: show stp instance


 ## CIST
Designated Root Bridge   00:00:00:00:00:00    Priority 0
                         We are the Root for CST
                         Port 0       , path cost 0
Regional Root Bridge     00:00:00:00:00:00    Priority  0
                        Path cost 0
```

```
Designated Bridge       00:00:00:00:00:00    Priority  0
Configured Forward delay 15, Max age 20, Max hops 20
Operational Forward delay 15, Max age 20
Topology Changes Count : 0
Last Topology Change     : 0

Interface Role       Sts       Cost    Prio.Nbr Type
------------ ------  ------    ------  ---------- -------

DGS-1210-28MP:5#
```

show stp mst_config_id

Purpose	To display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	The **show stp mst_config_id** command displays the Switch's current MSTP configuration identification.
Parameters	None.
Restrictions	None.

Example usage:

To show the MSTP configuration identification currently set on the Switch:

```
DGS-1210-28MP:5# show stp mst_config_id
Command: show stp mst_config_id


Name          [00:23:22:03:14:25]
Revision      0
Instance      Vlans mapped
 --------     ---------------------------------------------------------
 0            1-1024,1025-2048,2049-3072,3073-4094
 ------------------------------------------------------------------------

DGS-1210-28MP:5#
```

create stp instance_id

Purpose	To create instance ID on the Switch.
Syntax	**create stp instance_id <value 1-63>**
Description	The **create stp instance_id** command creates an instance ID of STP on the Switch.
Parameters	*<value 1-63>* - The value of the instance ID to be created.
Restrictions	Only administrator-level users can issue this command.

To create instance id 1:

```
DGS-1210-28MP:5# create stp instance_id 1
Command: create stp instance_id 1
```

```
Warning: There is no VLAN mapping to this instance_id!

Success.
DGS-1210-28MP:5#
```

delete stp instance_id

Purpose	To delete instance ID on the Switch.
Syntax	**delete stp instance_id <value 1-63>**
Description	The **delete stp instance_id** command removes the instance ID of STP on the Switch.
Parameters	*<value 1-63>* - The value of the instance ID to be removed.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To remove instance id 2:

```
DGS-1210-28MP:5# delete stp instance_id 1
Command: delete stp instance_id 1

Success.
DGS-1210-28MP:5#
```

config stp instance_id

Purpose	To configure instance ID on the Switch.
Syntax	**config stp instance_id <value 1-63> [add_vlan | remove_vlan] <vidlist>**
Description	The **config stp instance_id** command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.
Parameters	*<value 1-63>* − Enter a number between 1 and 15 to define the *instance_id*. The Switch supports 63 STP instances with one unchangeable default instance ID set as *0*. *add_vlan* – Along with the *vid_range* <*vidlist*> parameter, this command will add VIDs to the previously configured STP *instance_id.* *remove_vlan* − Along with the *vid_range* <*vidlist*> parameter, this command will remove VIDs to the previously configured STP *instance_id.* <*vidlist*> − Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DGS-1210-28MP:5# config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.
DGS-1210-28MP:5#
```

config stp mst_config_id

Purpose	To update the MSTP configuration identification.
Syntax	**config stp mst_config_id [revision_level <int 0-65535> | name <string 32>]**
Description	The **config stp mst_config_id** command uniquely identifies the MSTP configuration currently configured on the Switch. Information entered here is attached to BDPU packets as an identifier for the MSTP region to which it belongs. Switches having the same revision_level, name and identical vlans mapped for STP instance_ids are considered to be part of the same MSTP region.
Parameters	*revision_level <int 0-65535>*– The MSTP configuration revision number. The value may be between 0 and 65535. This value, along with the name and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. The default setting is 0. *name <string 32>* - A string of up to 32 alphanumeric characters to uniquely identify the MSTP region on the Switch. This name, along with the revision_level value and identical vlans mapped for STP instance_ids identifies the MSTP region configured on the Switch. If no name is entered, the default name is the MAC address of the device.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with revision_level 10 and the name 'Trinity':

```
DGS-1210-28MP:5# config stp mst_config_id name Trinity revision_level 10
Command: config stp mst_config_id name Trinity revision_level 10

Success.
DGS-1210-28MP:5#
```

config stp mst_ports

Purpose	To update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}**
Description	The **config stp mst_ports** command updates the port configuration for a STP instance_id. If a loop occurs, the MSTP function uses the port cost to select an interface to put into the forwarding state (if the switch isn't Root). If the switch is Root, then higher priority value for interfaces will influence on selected ports to be forwarding first at connected network devices. In instances where the priority value is identical, the MSTP function implements the lowest port number into the forwarding state and other interfaces are blocked. Remember that lower priority values mean higher priorities for forwarding

	packets.
Parameters	*<portlist>* – A port or range of ports to be configured. The port list is specified by listing switch number and the beginning port number on that switch, separated by a colon. Then the highest port number of the range is specified. The beginning and end of the port list range are separated by a dash. *instance_id <value 0-15>* - The value may be between 0 and 15. An entry of 0 denotes the CIST (Common and Internal Spanning Tree. *internalCost* – The relative cost of forwarding packets to specified ports when an interface is selected within an STP instance. The default setting is auto. There are two options: • *auto* – Specifies setting the quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. • *value 1-200000000* – Specifies setting the quickest route when a loop occurs. The value may be in the range of 1-200000000. A lower internalCost represents a quicker transmission. *priority <value 0-240>* - The priority for the port interface The value may be between 0 and 240. A lower number denotes a higher priority. A higher priority designates the interface to forward packets first.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To designate ports 1 through 5 with instance ID 2, to have an auto internalCost and a priority of 16:

```
DGS-1210-28MP:5# config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command: config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16

Success.

DGS-1210-28MP:5#
```

config stp trap

Purpose	To configure the sending state for STP traps.
Syntax	**config stp trap {new_root [enable | disable] | topo_change [enable | disable]}**
Description	The **config stp mst_ports** command is used to configure the sending state for STP traps.
Parameters	*new_root [enable | disable]* – Enable or disable sending of new root trap. The default state is enabled. *topo_change [enable | disable]* – Enable or disable sending of topology change trap. The default state is enabled.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure the new root and topo change to be enabled for STP trap:

```
DGS-1210-28MP:5# config stp trap new_root disable topo_change enable
Command: config stp trap new_root disable topo_change enable

Success.
DGS-1210-28MP:5#
```

config stp nni_bpdu_addr

Purpose	To configure destination MAC address for BPDU packets.
Syntax	**config stp nno_bpdu_addr [dot1d | dot1ad]**
Description	The **config stp nno_bpdu_addr** command is used choose the destination MAC address of BPDU packets that user desired.
Parameters	*dot1d* – Regular destination MAC address for 802.1d *dot1ad* – Detination MAC address (01:80:c2:00:00:08) that used for BPDU tunnel in QinQ scenario.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To configure BUDP address to dat1ad:

```
DGS-1210-28MP:5# config stp nni_bpdu_addr dot1ad
Command: config stp nni_bpdu_addr dot1ad

Success.

DGS-1210-28MP:5#
```

28

TIME AND SNTP COMMANDS

The Time and SNTP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config sntp	{primary [<ipaddr> | <ipv6addr>] | secondary [<ipaddr> | <ipv6addr>] | poll-interval <sec 30-99999>}
show sntp	
enable sntp	
disable sntp	
config time	<date> <systime>
config time_zone operator	[+ hour <gmt_hour 0-13> minute <minute 0-59> | - hour <gmt_hour 0-12> minute <minute 0-59>]
config dst	[disable | [annual s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <int 1-31> e_mth <end_mth 1-12> e_time <end_time> | offset [30 | 60 | 90 | 120]]]
show time	

Each command is listed in detail, as follows:

config sntp	
Purpose	To setup SNTP service.
Syntax	**config sntp {primary [<ipaddr> | <ipv6addr>] | secondary [<ipaddr> | <ipv6addr>] | poll-interval <sec 30-99999>}**
Description	The **config sntp** command configures SNTP service from an SNTP server. SNTP must be enabled for this command to function (See **enable sntp**).
Parameters	*primary [<ipaddr>| <ipv6addr>]* – Specifies the IPv4 or IPv6 address of the primary SNTP server. *secondary [<ipaddr>| <ipv6addr>]* – Specifies the IPv4 or IPv6 address of the secondary SNTP server. *poll-interval <sec 30-99999>* – The interval between requests for updated SNTP information. The polling interval ranges from 60 seconds (1 minute) to 86,400 seconds (1 day).
Restrictions	Only administrator or operate-level users can issue this command. SNTP service must be enabled for this command to function (*enable sntp*).

Example usage:

To configure SNTP settings:

```
DGS-1210-28MP:5# config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 60
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 60

Success.
DGS-1210-28MP:5#
```

show sntp

Purpose	To display the SNTP information.
Syntax	**show sntp**
Description	The **show sntp** command displays SNTP settings information, including the source IP address, time source and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DGS-1210-28MP:5# show sntp
Command: show sntp


SNTP Information
-----------------------------------------
Current Time Source          : Local
SNTP                         : Disabled
SNTP Primary Server          : 10.1.1.1
SNTP Secondary Server        : 10.1.1.2
SNTP Poll Interval           : 60 sec

DGS-1210-28MP:5#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	**enable sntp**
Description	The **enable sntp** command enables SNTP server support. SNTP service must be separately configured (see **config sntp**). Enabling and configuring SNTP support override any manually configured system time settings.
Parameters	None.
Restrictions	Only administrator and Operator-level users can issue this command. SNTP settings must be configured for SNTP to function (**config sntp**).

Example usage:

To enable the SNTP function:

```
DGS-1210-28MP:5# enable sntp
Command: enable sntp

Success.
DGS-1210-28MP:5#
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	**disable sntp**
Description	The **disable sntp** command disables SNTP support.
Parameters	None.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To disable SNTP support:

```
DGS-1210-28MP:5# disable sntp
Command: disable sntp

Success.
DGS-1210-28MP:5#
```

config time

Purpose	To manually configure system time and date settings.
Syntax	**config time <date> <systime>**
Description	The **config time date** command configures the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	<*date*> –Specifies the date, using two numerical characters for the day of the month, English abbreviation for the name of the month, and four numerical characters for the year. For example: 19jan2011. <*systime* > – Specifies the system time, using the format hh:mm:ss; that is, two numerical characters each for the hour using a 24-hour clock, the minute and second. For example: 19:42:30.
Restrictions	Only administrator or operate-level users can issue this command. Manually configured system time and date settings are overridden if SNTP support is enabled.

Example usage:

To manually set system time and date settings:

```
DGS-1210-28MP:5# config time 09jan2012 15:50:50
Command: config time 09jan2012 15:50:50

Success.
DGS-1210-28MP:5#
```

config time_zone operator	
Purpose	To determine the time zone used in order to adjust the system clock.
Syntax	**config time_zone operator [+ hour <gmt_hour 0-13> minute <minute 0-59> | - hour <gmt_hour 0-12> minute <minute 0-59>]**
Description	The **config time_zone operator** command adjusts the system clock settings according to the time zone. Time zone settings adjust SNTP information accordingly.
Parameters	*operator* – May be (+) to add or (-) to subtract time to adjust for time zone relative to GMT. *hour <gmt_hour 0-13>* – Specifies the number of hours difference from GMT. *minute <minute 0-59>* – Specifies the number of minutes added or subtracted to adjust the time zone.
Restrictions	Only administrator or operator level users can issue this command.

Example usage:

To configure time zone settings:

```
DGS-1210-28MP:5# config time_zone operator + hour 2 minute 30
Command: config time_zone operator + hour 2 minute 30

Success.
DGS-1210-28MP:5#
```

config dst	
Purpose	To configure time adjustments to allow for the use of Daylight Saving Time (DST).
Syntax	**config dst [disable | [annual s_date <start_date 1-31> s_mth <start_mth 1-12> s_time <start_time> end_date <int 1-31> e_mth <end_mth 1-12> e_time <end_time> | offset [30 | 60 | 90 | 120]]]**
Description	The **config dst** command disables or configures Daylight Saving Time (DST). When enabled, this adjusts the system clock to comply with any DST requirement. DST adjustment affects system time for both manually configured time and time set using SNTP service.
Parameters	*disable* – Disables the DST seasonal time adjustment for the Switch. *annual* – Enables DST seasonal time adjustment on an annual basis. Annual mode requires that the DST beginning and ending date be specified concisely. For example, specify to begin DST on April 3 and end DST on October 14. The format for annual mode is as follows, and in the order listed: • *s_date <start_date 1-31>* - The day of the month to begin DST, expressed numerically. • *s_mth <start_mth 1-12>* - The month of the year to begin DST, expressed numerically. • *s_time <start_time>* - The time of day to begin DST in hours and minutes, expressed using a 24-hour clock. • *end_date <int 1-31>* - The day of the month to end DST, expressed numerically. • *e_mth <end_mth 1-12>* - The month of the year to end DST,

	expressed numerically. • *e_time<end_time>* - The time of day to end DST, in hours and minutes, expressed using a 24-hour clock. *offset [30 | 60 | 90 | 120]* – Indicates the number of minutes to add during the summertime. The possible offset times are 30, 60, 90, and 120. The default value is 60.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch to run from the 2nd Tuesday in April at 3 PM until the 2nd Wednesday in October at 3:30 PM and add 30 minutes at the onset of DST:

```
DGS-1210-28MP:5# config dst annual s_date 2 s_mth 4 s_time 3 end_date 2
e_mth 10 e_time 3 offset 30
Command: config dst annual s_date 2 s_mth 4 s_time 3 end_date 2 e_mth 10
e_time 3 offset 30



Success.
DGS-1210-28MP:5#
```

show time

Purpose	To display the current time settings and status.
Syntax	**show time**
Description	The **show time** command displays the system time and date configuration, as well as displays the current system time.
Parameters	None.
Restrictions	None.

Example usage:

To show the time cuurently set on the Switch's System clock:

```
DGS-1210-28MP:5# show time
Command: show time

Time information
--------------------------------------------------------------------------------
Current Time Source              : Local
Current Time                     : 09 Jan 2012 15:56:02
GMT Time Zone offset             : GMT +02:30
Daylight Saving Time Status      : Annual
Offset in Minutes                : 60
Annual From                      : 01 Jan 0:0
To                               : 01 Jan 0:0

DGS-1210-28MP:5#
```

29

ARP COMMANDS

The ARP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config arp_aging time	<value 0-65535 >
clear arptable	
create arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> | all]
show arpentry	{information | interface_name {system} | ip_address <ipaddr> | mac_address <macaddr> | summary | static}
show arpentry aging_time	

Each command is listed in detail, as follows:

config arp_aging time	
Purpose	To configure the age-out timer for ARP table entries on the Switch.
Syntax	**config arp_aging time <value 0-65535>**
Description	The **config arp_aging time** command sets 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	*<value 0-65535>* – The ARP age-out time, in minutes. The value may be in the range of 0-65535 minutes, with a default setting of 20 minutes.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ARP aging time:

```
DGS-1210-28MP:5# config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-1210-28MP:5#
```

clear arptable

Purpose	To remove all dynamic ARP table entries.
Syntax	**clear arptable**
Description	The **clear arptable** command is used to remove dynamic ARP table entries from the Switch's ARP table. Static ARP table entries are not affected.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To remove dynamic entries in the ARP table:

```
DGS-1210-28MP:5# clear arptable
Command: clear arptable

Success.

DGS-1210-28MP:5#
```

create arpentry

Purpose	To create an entry for ARP table on the Switch.
Syntax	**create arpentry <ipaddr> <macaddr>**
Description	The **create arpentry <ipaddr> <macaddr>** command is used to create an entry for ARP table on the Switch.
Parameters	*<ipaddr>* – Specify the IP address to be configured. *<macaddr>* – Specify the MAC address to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create an ARP entry:

```
DGS-1210-28MP:5# create arpentry 10.90.90.94 00-00-00-01-02-03
Command: create arpentry 10.90.90.94 00-00-00-01-02-03


Success.

DGS-1210-28MP:5#
```

config arpentry	
Purpose	To configure the entry for ARP table on the Switch.
Syntax	**config arpentry <ipaddr> <macaddr>**
Description	The **config arpentry** command is used to configure the entry for ARP table on the Switch.
Parameters	*<ipaddr>* – Specify the IP address to be configured. *<macaddr>* – Specify the MAC address to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure ARP entry:

```
DGS-1210-28MP:5# config arpentry 10.90.90.94 00-00-00-01-02-05
Command: config arpentry 10.90.90.94 00-00-00-01-02-05



Success.

DGS-1210-28MP:5#
```

delete arpentry	
Purpose	To remove the entry for ARP table on the Switch.
Syntax	**delete arpentry [<ipaddr> | all]**
Description	The **delete arp_aging time** command is used to configure the entry for ARP table on the Switch.
Parameters	*[<ipaddr> | all]* – Specifiy the IP address or all of ARP entry to be removed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To remove the ARP entry:

```
DGS-1210-28MP:5# delete arpentry 10.90.90.94
Command: delete arpentry 10.90.90.94



Success.

DGS-1210-28MP:5#
```

show arpentry	
Purpose	To displays all ARP entries on the Switch.
Syntax	**show arpentry {information | interface_name {system} | ip_address <ipaddr> | mac_address <macaddr> | summary | static}**
Description	The **show arpentry** command displays all ARP entries on the Switch.
Parameters	*information* – Displays the information of ARP entry. *interface_name {system}* – Displays the interface name of ARP entry. *ip_address <ipaddr>* – Displays the IP address of ARP entry. *mac_address<macaddr>* – Displays the MAC address of ARP entry. *summary* – Displays the summary of ARP entry. *static* – Display static ARP entry
Restrictions	None.

Example usage:

To display all ARP entries information on the Switch:

```
DGS-1210-28MP:5# show arpentry information
Command: show arpentry information


ARP Configurations:
--------------------
 Maximum number of ARP request retries is 3
 ARP cache timeout is 1800 seconds

DGS-1210-28MP:5#
```

show arpentry aging_time	
Purpose	To displays the ARP entry aging time on the Switch.
Syntax	**show arpentry aging_time**
Description	The **show arpentry aging_time** command displays the ARP entry aging time on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the ARP entry aging time on the Switch:

```
DGS-1210-28MP:5# show arpentry aging_time
Command: show arpentry aging_time

ARP Aging Time = 30 (minutes)

DGS-1210-28MP:5#
```

30

IPV6 NEIGHBOR DISCOVERY COMMANDS

The IPv6 Neighbor Discovery commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create ipv6 neighbor_cache ipif	System <ipv6_addr> <mac_addr>
delete ipv6 neighbor_cache	[<ipv6_addr> | static | dynamic | all]
show ipv6 neighbor_cache	[ipv6address <ipv6_addr> | static | dynamic | all]
config ipv6 nd ns ipif	System retrans_time <integer 1-3600>
show ipv6 nd	
create ipv6route default	<ipv6addr>
delete ipv6route default	
show ipv6route	
enable ipif_ipv6_link_local_auto System	
disable ipif_ipv6_link_local_auto System	
enable ipv6 nd flooding	
disable ipv6 nd flooding	

Each command is listed in detail, as follows:

create ipv6 neighbor_cache ipif	
Purpose	Used to add a static neighbor on an IPv6 interface.
Syntax	**create ipv6 neighbor_cache ipif System <ipv6_addr> <mac_addr>**
Description	This **create ipv6 neighbor_cache ipif** command is used to add a static neighbor on an IPv6 interface.
Parameters	<*ipv6_addr*> –The IPv6 address of the neighbor. <*mac_addr*> –The MAC address of the neighbor.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a static neighbor cache entry on the interface System, with an IPv6 address of 3ffc::1 and a MAC address of 00:01:02:03:04:05:

```
DGS-1210-28MP:5# 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-1210-28MP:5#
```

delete ipv6 neighbor_cache

Purpose	Used to remove a static neighbor on an IPv6 interface.
Syntax	**delete ipv6 neighbor_cache [<ipv6_addr> | static | dynamic | all]**
Description	This **delete ipv6 neighbor_cache ipif** command is used to remove a static neighbor on an IPv6 interface.
Parameters	*<ivp6_addr>* –The IPv6 address of the neighbor. *static* – Delete matching static entries. *dynamic* – Delete matching dynamic entries. *all* – All entries including static and dynamic entries will be deleted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a static neighbor cache entry on the interface System, with an IPv6 address of 3ffc::1:

```
DGS-1210-28MP:5# delete ipv6 neighbor_cache 3ffc::1
Command: delete ipv6 neighbor_cache 3ffc::1

Success.
DGS-1210-28MP:5#
```

show ipv6 neighbor_cache

Purpose	Used to display the IPv6 neighbor cache.
Syntax	**show ipv6 neighbor_cache [ipv6address <ipv6_addr> | static | dynamic | all]**
Description	This **show ipv6 neighbor_cache ipif** command is used to display the neighbor cache entry for the specified interface. You can display a specific entry, all static entries, all dynamic entries, or all entries.
Parameters	*ipv6address <ipv6_addr>* –The IPv6 address of the neighbor. *static* – Display all static neighbor cache entries. *dynamic* – Display all dynamic entries. *all* – Displays all entries including static and dynamic entries.
Restrictions	None.

Example usage:

To show all neighbor cache entries on the switch:

```
DGS-1210-28MP:5#  show ipv6 neighbor_cache ipif all static
Command: show ipv6 neighbor_cache ipif all static


   IPv6 Address              Link-layer Addr     State     Interface
   ------------------        ----------------------  ---------  ---------

Total Entries: 0

DGS-1210-28MP:5#
```

config ipv6 nd ns ipif

Purpose	Configures the IPv6 ND neighbor solicitation retransmit time，which is the time between the retransmission of neighbor solicitation messages to a neighbor, when resolving the address or when probing the reachability of a neighbor.
Syntax	**config ipv6 nd ns ipif System retrans_time <integer 1-3600>**
Description	This **config ipv6 neighbor_cache ipif** command is used to configures the retransmit time of IPv6 ND neighbor solicitation
Parameters	*retrans_time <integer 1 - 3600>* – Neighbor solicitation's retransmit timer in milliseconds. It has the same value as the RA retrans_time in the config IPv6 ND RA command. If the retrans_time parameter is configured in one of the commands, the retrans_time value in the other command will also change so that the values in both commands are the same. The range if 1 to 3600.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the retrans_time of IPv6 ND neighbor solicitation to be 100:

```
DGS-1210-28MP:5# config ipv6 nd ns ipif System retrans_time 100
Command: config ipv6 nd ns ipif System retrans_time 100

Success.
DGS-1210-28MP:5#
```

show ipv6 nd

Purpose	Used to display information regarding neighbor detection on the switch.
Syntax	**show ipv6 nd**
Description	This **show ipv6 nd** command is used to display information regarding neighbor detection on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show IPv6 ND related configuration:

```
DGS-1210-28MP:5#  show ipv6 nd
Command: show ipv6 nd

Interface Name              : System
NS Retransmit Time          : 1(ms)

DGS-1210-28MP:5#
```

create ipv6route default

Purpose	Used to create IPv6 route entries to the Switch's IP routing table.
Syntax	**create ipv6route default <ipv6addr>**
Description	This **create ipv6route default** command is used to create a primary and backup IP route entry to the Switch's IP routing table.
Parameters	*<ipv6addr>* – Specify the IPv6 address to be crete.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To add a single static IPv6 entry in IPv6 format:

```
DGS-1210-28MP:5# create ipv6route default 3ffc::1
Command: create ipv6route default 3ffc::1

Success.
DGS-1210-28MP:5#
```

delete ipv6route default

Purpose	Used to delete a static IPv6 route entry from the Switch's IP routing table.
Syntax	**delete ipv6route default**
Description	This **delete ipv6route default** command will delete an existing static IPv6 entry from the Switch's IP routing table.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To o delete a static IPv6 entry from the routing table:

```
DGS-1210-28MP:5# delete ipv6route default
Command: delete ipv6route default

Success.
DGS-1210-28MP:5#
```

show ipv6route

Purpose	Used to display IPv6 routes.

Syntax	**show ipv6route**
Description	This **show ipv6route** command displays the IPv6 routes.
Parameters	None.
Restrictions	None.

Example usage:

To show IPv6 route:

```
DGS-1210-28MP:5#  show ipv6route
Command: show ipv6route

Prefix        Next Hop                 IP Interface      Protocol
Metric
------        --------                 ------------      --------
 ------
::/01         3ffc::1                   System           Static



Total Entries: 1

DGS-1210-28MP:5#
```

enable ipif_ipv6_link_local_auto System

Purpose	Used to enable the autoconfiguration of the link local address when no IPv6 address is configured.
Syntax	**enable ipif_ipv6_link_local_auto System**
Description	This **enable ipif_ipv6_link_local_auto System** command will automatically create an IPv6 link local address for the Switch if no IPv6 address has previously been configured.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the IP interface IPv6 link-local settings on the switch:

```
DGS-1210-28MP:5# enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System

Success.
DGS-1210-28MP:5#
```

disable ipif_ipv6_link_local_auto System

Purpose	Used to disable the autoconfiguration of the IPv6 link local address.
Syntax	**disable ipif_ipv6_link_local_auto System**
Description	This **disable ipif_ipv6_link_local_auto System** command will

	disable the automatic creation of an IPv6 link local address for the Switch. Once this command is entered, any previous IPv6 link local address that has been created for the IP interface selected will be deleted from the switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the IP interface IPv6 link-local settings on the switch:

```
DGS-1210-28MP:5# disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.
DGS-1210-28MP:5#
```

enable ipv6 nd flooding

Purpose	Used to enable the flood mechanism for Neighbor Discovery packets.
Syntax	**enable ipv6 nd flooding**
Description	This **enable ipv6 nd flooding** command is used to enable the flood mechanism for Neighbor Discovery packets.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the ND flooding:

```
DGS-1210-28MP:5# enable ipv6 nd flooding
Command: enable ipv6 nd flooding

Success.

DGS-1210-28MP:5#
```

disable ipv6 nd flooding

Purpose	Used to disable the flood mechanism for Neighbor Discovery packets.
Syntax	**disable ipv6 nd flooding**
Description	This **disable ipv6 nd flooding** command is used to disable the flood mechanism for Neighbor Discovery packets.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the ND flooding:

```
DGS-1210-28MP:5# disable ipv6 nd flooding
Command: disable ipv6 nd flooding


Success.

DGS-1210-28MP:5#
```

31

BANNER COMMANDS

The Banner commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config log_save_timing	[log_trigger | on_demand | time_interval <minutes 1-65535>]
show log_save_timing	
show log	{index <indexlist> | module <string 32> | severity [warning | all | informational]}

Each command is listed in detail, as follows:

config log_save_timing	
Purpose	Used to configure the method of saving logs to the Switch's Flash memory.
Syntax	**config log_save_timing [log_trigger | on_demand | time_interval <minutes 1-65535>]**
Description	This **config log_save_timing** command is used to configure the method used in saving logs to the Switch's Flash memory.
Parameters	*log_trigger* – Users who choose this method will have logs saved to the Switch every time a log event occurs on the Switch. *on_demand* – Users who choose this method will only save logs when they manually tell the Switch to do so, using the save all or save log command. *time_interval <minutes 1-65535>* – Use this parameter to configure the time interval that will be implemented for saving logs. The logs will be saved every x number of minutes that are configured here.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the time interval as every 30 minutes for saving logs:

```
DGS-1210-28MP:5# config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success.

DGS-1210-28MP:5#
```

show log_save_timing

Purpose	Used to show the log save timing.
Syntax	**show log_save_timing**
Description	This command allows display of the log save timing on the Switch.
Parameters	None.
Restrictions	None.

Usage Example:

To show the login banner:

```
DGS-1210-28MP:5# show log_save_timing
Command: show log_save_timing

Saving log method: time_interval
                   Interval : 100

DGS-1210-28MP:5#
```

show log

Purpose	Used to show the log.
Syntax	**show log {index <indexlist> | module <string 32> | severity [warning | all | informational]}**
Description	This command allows display the log.
Parameters	*index <indexlist>* – Specifies the index of logs to be displayed. *module <string 32>* – Specifies the module of logs to be displayed. *severity [warning | all | informational]* – Specifies the severity of logs to be displayed.
Restrictions	None.

Usage Example:

To show the log index 1 on the Switch:

```
DGS-1210-28MP:5# show log index 1
Command: show log index 1

Index  Time              Log Text
-----  ----------------- ----------------------------------------
 1     Jan  1 00:00:16:SYSTEM-6:Side Fan is in low speed.



DGS-1210-28MP:5#
```

32

COMMAND HISTORY LIST COMMANDS

The Command History List commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
?	
config command_history	<value (1-40)>
show command_history	
enable command logging	
disable command logging	
show command logging	

Each command is listed in detail, as follows:

?	
Purpose	To display all commands in the Command Line Interface (CLI).
Syntax	**?**
Description	The **?** command displays all of the commands available through the Command Line Interface (CLI).
Parameters	*{<command>}* – Lists all the corresponding parameters for the specified command, along with a brief description of the command's function and similar commands having the same words in the command.
Restrictions	None.

Example usage:

To display all of the commands in the CLI:

```
DGS-1210-28MP:5# ?
Command: ?


USEREXEC commands :
?
boot imageid
cable diagnostic port
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear counters
clear ethernet_oam ports
clear fdb
clear flood_fdb
clear igmp_snooping data_driven_group
clear igmp_snooping statistics counter
clear log
clear mld_snooping statistics counter
clear port_security_entry port
clear tech support
compute dlink-SHA1
config 802.1x auth_mode
config 802.1x auth_parameter portsCTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

show command_history

Purpose	To display the command history.
Syntax	**show command_history**
Description	The **show command_history** command displays the command history.
Parameters	None.
Restrictions	None.

Example usage:

To display the command history:

```
DGS-1210-28MP:5# show command_history
Command: show command_history

?
show log
show log_save_timing
show log_save_timing

DGS-1210-28MP:5#
```

enable command logging

Purpose	To enable loging the command issued.
Syntax	**enable command logging**
Description	The **enable command logging** command is used to logging the command issued.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable command logging:

```
DGS-1210-28MP:5# enable command logging
Command: enable command logging


Success.

DGS-1210-28MP:5#
```

disable command logging

Purpose	To disable command logging mechanism.
Syntax	**disable command logging**
Description	The **disable command logging** command is used to turn off command logging feature.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable command logging:

```
DGS-1210-28MP:5# disable command logging
Command: disable command logging


Success.

DGS-1210-28MP:5#
```

show command logging

Purpose	To display command logging mechanism.
Syntax	**show command logging**
Description	The **show command logging** command is used to display command logging feature current state
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To show command logging:

```
DGS-1210-28MP:5# show command logging
Command: show command logging

Command Logging State : Enabled

DGS-1210-28MP:5#
```

33

ACCESS AUTHENTICATION CONTROL COMMANDS

The Access Authentication Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method [radius | local | server_group <string 15> | none]
delete authen_login method_list_name	<string 15>
show authen_login	[all | default | method_list_name <string 15>]
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {radius | local | server_group <string 15> | none}
delete authen_enable method_list_name	<string 15>
show authen_enable	[all | default | method_list_name <string 15>]
enable authen_policy	
disable authen_policy	
show authen_policy	
config authen application	[console | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
config authen parameter	[attempt <int 1-255> | response_timeout <int 0-255>]
show authen parameter	
create authen server_host	[<ipaddr>| <ipv6addr>] protocol radius {port <int 1-65535> | key <string 254> | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	[<ipaddr> | <ipv6addr>] protocol radius {port <int 1-65535> | key [<string 254>] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	[<ipaddr> | <ipv6addr>] protocol radius
show authen server_host	
create authen	<string 15>

Command	Parameter
server_group	
config authen server_group	[<string 15> | radius] [add | delete] server_host [<ipaddr> | <ipv6addr>] protocol radius
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
enable admin	

Each command is listed in detail, as follows:

create authen_login method_list_name

Purpose	To create a user-defined list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	The **create authen_login method_list_name** command creates a list of authentication techniques for user login. The Switch can support up to eight method lists, but one is reserved as a default and cannot be deleted. Multiple method lists must be created and configured separately.
Parameters	*<string 15>* - Defines the *method_list_name* to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create the method list 'Trinity':

```
DGS-1210-28MP:5# create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.
DGS-1210-28MP:5#
```

config authen_login

Purpose	To configure a user-defined or default *method list* of authentication methods for user login.
Syntax	**config authen_login [default | method_list_name <string 15>] method [radius | local | server_group <string 15> | none]**
Description	The **config authen_login** command configures a user-defined or default *method list* of authentication methods for users logging on to the Switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like *tacacs – local,* the Switch sends an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch sends an authentication request to the second *tacacs* host in the server group

	and so on, until the list is exhausted. When the local method is used, the privilege level is dependant on the local account privilege configured on the Switch. Successful login using any of these methods gives the user a 'user' priviledge only. If the user wishes to upgrade his or her status to the administrator level, the user must implement the *enable admin* command, followed by a previously configured password. (*See the **enable admin** part of this section for more detailed information, concerning the **enable admin** command.)*
Parameters	*default* – The default method list for access authentication, as defined by the user. The user may choose one or more of the following authentication methods: ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *server_group* <*string 15*> –Specifies that the user is to be authenticated using the server group *account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch. *method_list_name* <*string 15*> – Specifies a previously created method list name defined by the user. One or more of the following authentication methods may be added to this method list: ▪ *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. ▪ *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. ▪ *server_group* <*string 15*> –Specifies that the user is to be authenticated using the server group *account* database on the Switch. ▪ *none* – Specifies that no authentication is required to access the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the user defined method list 'Trinity' with authentication methods RADIUS and local, in that order.

```
DGS-1210-28MP:5# config authen_login method_list_name Trinity method radius local
Command: config authen_login method_list_name Trinity method radius local

Success.
DGS-1210-28MP:5#
```

delete authen_login method_list_name

Purpose	To delete a previously configured user defined list of authentication methods for users logging on to the Switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	The **delete authen_login method_list_name** command deletes a list of authentication methods for user login.

Parameters	<*string 15*> - The previously created *method_list_name* to delete.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete the method list name 'Trinity':

```
DGS-1210-28MP:5# delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.
DGS-1210-28MP:5#
```

show authen_login

Purpose	To display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**show authen_login [all | default | method_list_name <string 15>]**
Description	The **show authen_login** command displays a list of authentication methods for user login.
Parameters	*default* – Displays the default method list for users logging on to the Switch. *method_list_name* <*string 15*> - Specifies the *method_list_name* to display. *all* – Displays all the authentication login methods currently configured on the Switch. • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.
Restrictions	None.

Example usage:

To view all authentication login method list names:

```
DGS-1210-28MP:5#  show authen_login all
Command: show authen_login all

Method List Name Priority Method Name     Comment
------------------------ ---------- -------------------  ------------------
Trinity                  1          none                 Keyword
Trinity                  2          none                 Keyword
Trinity                  3          none                 Keyword
Trinity                  4          none                 Keyword

------------------------ ---------- -------------------  ------------------
default                  1          local                Keyword
default                  2          none                 Keyword
default                  3          none                 Keyword
default                  4          none                 Keyword

DGS-1210-28MP:5#
```

create authen_enable method_list_name

Purpose	To create a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**create authen_enable method_list_name <string 15>**
Description	The **create authen_enable method_list_name** command creates a list of authentication methods for promoting users with normal level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented on the Switch.
Parameters	*<string 15>* - Defines the *authen_enable method_list_name* to be created as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a user-defined method list, named ‘Permit’ for promoting user privileges to Adminstrator privileges:

```
DGS-1210-28MP:5# create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.
DGS-1210-28MP:5#
```

config authen_enable

Purpose	To configure a user-defined method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.

Syntax	**config authen_enable [default | method_list_name <string 15>] method {radius | local | server_group <string 15> | none}**
Description	The **config authen_enable** command configures a user-defined list of authentication methods for promoting normal user level privileges to Administrator level privileges using authentication methods on the Switch. Once a user acquires normal user level privileges on the Switch, he or she must be authenticated by a method on the Switch to gain administrator privileges on the Switch, which is defined by the Administrator. A maximum of eight (8) enable method lists can be implemented simultaneously on the Switch. The sequence of methods implemented in this command affects the authentication result. For example, if a user enters a sequence of methods like *radius* – *local_enable,* the Switch sends an authentication request to the first RADIUS host in the server group. If no verification is found, the Switch sends an authentication request to the second RADIUS host in the server group and so on, until the list is exhausted. At that point, the Switch restarts the same sequence with the following protocol listed, *radius*. If no authentication takes place using the *radius* list, the *local_enable* password set in the Switch is used to authenticate the user. Successful authentication using any of these methods gives the user an 'Admin' level privilege.
Parameters	*default* – The default method list for adminstration rights authentication, as defined by the user. The user may choose one or more of the following authentication methods: • *radius* – Specifies that the user is to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. • *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. • *server_group* <*string 15*> – Specifies the server group name for authentication. • *none* – Specifies that no authentication is required to access the Switch. *method_list_name* <*string 15*> – Specifies a previously created *authen_enable method_list_name*. The user may add one or more of the following authentication methods to this method list: • *radius* - Specifies that the user is to be authenticated using the *RADIUS* protocol from a remote RADIUS server. • *local* - Specifies that the user is to be authenticated using the local *user account* database on the Switch. The local enable password of the device can be configured using the '**config admin local_password**' command. • *server_group* <*string 15*> –Specifies that the user is to be authenticated using the server group account database on the Switch. • *none* – Specifies that no authentication is required to access the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the user defined method list 'Permit' with authentication methods RADIUS and local_enable, in that order.

```
DGS-1210-28MP:5# config authen_enable method_list_name Trinity method
radius local
Command: config authen_enable method_list_name Trinity method  radius local

Success.
DGS-1210-28MP:5#
```

delete authen_enable method_list_name

Purpose	To delete a user-defined list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**delete authen_enable method_list_name <string 15>**
Description	The **delete authen_enable method_list_name** command deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.
Parameters	*<string 15>* - The previously created *authen_enable method_list_name* to be deleted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete the user-defined method list 'Permit'

```
DGS-1210-28MP:5# delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.
DGS-1210-28MP:5#
```

show authen_enable

Purpose	To display the list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**show authen_enable [all | default | method_list_name <string 15>]**
Description	The **show authen_enable** command deletes a user-defined list of authentication methods for promoting user level privileges to Adminstrator level privileges.
Parameters	*default* – Displays the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name <string 15>* – The *method_list_name* to be displayed. *all* – Displays all the authentication login methods currently configured on the Switch. The command displays the following parameters: • Method List Name – The name of a previously configured method list name. • Method Name – Defines which security protocols are implemeted, per method list name.
Restrictions	None.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DGS-1210-28MP:5# show authen_enable all
Command: show authen_enable all

Method List Name  Priority  Method Name   Comment
------------------------  --------  ------------------  ------------------
default                   1         local               Keyword

DGS-1210-28MP:5#
```

enable authen_policy

Purpose	To enable the authentication policy on the Switch.
Syntax	**enable authen_policy**
Description	The **enable authen_policy** command enables the authentication policy on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the authentication policy:

```
DGS-1210-28MP:5# enable authen_policy
Command: enable authen_policy

Success.
DGS-1210-28MP:5#
```

disable authen_policy

Purpose	To disable the authentication policy on the Switch.
Syntax	**disable authen_policy**
Description	The **disable authen_policy** command disables the authentication policy on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the authentication policy:

```
DGS-1210-28MP:5# disable authen_policy
Command: disable authen_policy

Success.
DGS-1210-28MP:5#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	**show authen_policy**
Description	The **show authen_policy** command display the system access authentication policy status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the system access authentication policy:

```
DGS-1210-28MP:5# show authen_policy
Command: show authen_policy

Authentication Policy : Disabled
DGS-1210-28MP:5#
```

config authen application

Purpose	To configure various applications on the Switch for authentication using a previously configured method list.
Syntax	**config authen application [console | http | all] [login | enable] [default | method_list_name <string 15>]**
Description	The **config authen application** command configures Switch applications (console, Telnet) for login at the user level and at the administration level (*authen_enable*), utilizing a previously configured method list.
Parameters	*application* – Specifies the application to configure. One of the following four options may be selected: • *console* – Configures the command line interface login method. • *http* – Configures the http login method. • *all* – Configures all applications as (console, Telnet, SSH) login methods. *login* – Configures an application for normal login on the user level, using a previously configured method list. *enable* – Configures an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Configures an application for user authentication using the default method list. *method_list_name* <*string 15*> – Configures an application for user authentication using a previously configured *method_list_name*.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DGS-1210-28MP:5# config authen application http login default
Command: config authen application http login default

Success.
DGS-1210-28MP:5#
```

show authen application

Purpose	To display authentication methods for the various applications on the Switch.
Syntax	**show authen application**
Description	The **show authen application** command displays all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, Telnet, SSH) currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the login and enable method list for all applications on the Switch:

```
DGS-1210-28MP:5#  show authen application
Command: show authen application

Application  Login Method List   Enable Method List
---------- ---------------------------- ------------------------------
Telnet       default              default
HTTP         default              default

DGS-1210-28MP:5#
```

config authen parameter

Purpose	To provide user to configure the authentication parameters on the Switch.
Syntax	**config authen parameter [attempt <int 1-255> | response_timeout <int 0-255>]**
Description	The **config authen parameter attempt** command provides user to configure the authentication parameters on the Switch.
Parameters	*attemtp <integer 1-255>* – Specifies the attempt of authentication parameter on the Switch. The value range is between 1 and 255. *response_timout <integer 0-255>* – Specifies the response timout of authentication parameter on the Switch. The value range is between 0 and 255.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the default method list for the command line interface:

```
DGS-1210-28MP:5# config authen parameter attempt 10
Command: config authen parameter attempt 10

Success.
DGS-1210-28MP:5#
```

show authen parameter

Purpose	To display authentication parameters for the various applications on the Switch.
Syntax	**show authen parameter**
Description	The **show authen parameter** command displays the authentication parameter on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the authentication parameters for all applications on the Switch:

```
DGS-1210-28MP:5# show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 10 times
DGS-1210-28MP:5#
```

create authen server_host

Purpose	To create an authentication server host.
Syntax	**create authen server_host [<ipaddr>| <ipv6addr>] protocol radius {port <int 1-65535> | key <string 254> | timeout <int 1-255> | retransmit <int 1-255>}**
Description	The **create authen server_host** command creates an authentication server host for the RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch sends authentication packets to a remote RADIUS server host on a remote host. The RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that RADIUS is separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*<ipaddr>* – The IPv4 address of the remote server host to add. *<ipv6addr>* – The IPv6 address of the remote server host to add. *protocol radius* – Specifies that the server host utilizes the RADIUS protocol. *port <int 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port numbers are 1812 and 1813 for RADIUS servers

	but the user may set a unique port number for higher security. *key [<string 254>]* – The authentication key to be shared with a configured RADIUS server only. The value is a string of up to 254 alphanumeric characters. *timeout <int 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a RADIUS authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

```
DGS-1210-28MP:5#  create authen server_host 10.1.1.121 protocol radius port 1234 timeout 10 retransmit 5
Command: create authen server_host 10.1.1.121 protocol radius port 1234 timeout10 retransmit 5

Success.
DGS-1210-28MP:5#
```

config authen server_host

Purpose	To configure a user-defined authentication server host.
Syntax	**config authen server_host [<ipaddr> | <ipv6addr>] protocol radius {port <int 1-65535> | key [<string 254>] | timeout <int 1-255> | retransmit <int 1-255>}**
Description	The **config authen server_host** command configures a user-defined authentication server host for the RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote RADIUS server host on a remote host. The RADIUS server host then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that RADIUS is separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*<ipaddr>* – The IPv4 address of the remote server host the user wishes to alter. *<ipv6addr>* – The IPv6 address of the remote server host the user wishes to alter *protocol radius* – Specifies that the server host utilizes the RADIUS protocol. *port <int 1-65535>* – The virtual port number of the authentication protocol on a server host. The value must be between 1 and 65535. The default port numbers are 1812 and 1813 for RADIUS servers but the user may set a unique port number for higher security. *key [<string 254>]* – The authentication key to be shared with a configured RADIUS server only. The value is a string of up to 254

	alphanumeric characters. *timeout <int 1-255>* – The time in seconds the Switch waits for the server host to reply to an authentication request. The default value is 5 seconds. *retransmit <int 1-255>* – The number of times the device resends an authentication request when the server does not respond. The value is between 1 and 255.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure a RADIUS authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DGS-1210-28MP:5# config authen server_host 10.1.1.121 protocol radius port 4321 timeout 12 retransmit 4
Command: config authen server_host 10.1.1.121 protocol radius port 4321 timeout 12 retransmit 4

Success.
DGS-1210-28MP:5#
```

delete authen server_host

Purpose	To delete a user-defined authentication server host.
Syntax	**delete authen server_host [<ipaddr> | <ipv6addr>] protocol radius**
Description	The **delete authen server_host** command deletes a user-defined authentication server host previously created on the Switch.
Parameters	*<ipaddr>* - The IPv4 address of the remote server host to be deleted. *<ipv6addr>* - The IPv6 address of the remote server host to be deleted. *protocol radius* – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a user-defined RADIUS authentication server host:

```
DGS-1210-28MP:5# delete authen server_host 10.1.1.121 protocol radius
Command: delete authen server_host 10.1.1.121 protocol radius

Success.
DGS-1210-28MP:5#
```

show authen server_host

Purpose	To view a user-defined authentication server host.
Syntax	**show authen server_host**
Description	The **show authen server_host** command displays user-defined

	authentication server hosts previously created on the Switch. The following parameters are displayed: IP Address – The IPv4 or IPv6 address of the authentication server host. Protocol – The protocol used by the server host. Port – The virtual port number on the server host. The default value is 49. Timeout - The time in seconds the Switch waits for the server host to reply to an authentication request. Retransmit - The value in the retransmit field denotes how many times the device resends an authentication request. Key - Authentication key to be shared with a configured RADIUS server only.
Parameters	None.
Restrictions	None.

Example usage:

To view authenticaion server hosts currently set on the Switch:

```
DGS-1210-28MP:5#  show authen server_host
Command: show authen server_host

IP Address  : 10.90.90.97
Protocol    : radius
Port        : 10
Timeout     : 2
Retransmit  : 5
Key         : kdjfl


Total Entries: 1
DGS-1210-28MP:5#
```

create authen server_group

Purpose	To create an authentication server host.
Syntax	**create authen server_group <string 15>**
Description	The **create authen server_ group** command creates an authentication server group for the protocols on the Switch.
Parameters	*<string 15>* – Defines the authentication group name as a string of up to 15 alphanumeric characters.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create a server group “dlinkgroup”:

```
DGS-1210-28MP:5# create authen server_group dlinkgroup
Command: create authen server_group dlinkgroup

Success.
DGS-1210-28MP:5#
```

config authen server_group

Purpose	To configure a user-defined authentication server host.
Syntax	**config authen server_group [<string 15> | radius] [add | delete] server_host [<ipaddr> | <ipv6addr>] protocol radius**
Description	The **config authen server_ group** command configures a user-defined authentication server group for the RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch sends authentication packets to a remote RADIUS server group on a remote host. The RADIUS server group then verifies or denies the request and returns the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that RADIUS is separate entities and are not compatible with each other. The maximum supported number of server group is 16.
Parameters	*<string 15>* – Defines the authentication group name as a string of up to 15 alphanumeric characters. *<ipaddr>* – The IPv4 address of the remote server group the user wishes to alter. *<ipv6addr>* – The IPv6 address of the remote server group the user wishes to alter. *[add | delete]* –Specifies the authentication server host will be add or deleted of the server group. *protocol radius* – Specifies that the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure a RADIUS authentication server group:

```
DGS-1210-28MP:5# config authen server_group dlinkgroup add server_host
10.1.1.121 protocol radius
Command: config authen server_group dlinkgroup add server_host 10.1.1.121
protocol radius

Success.
DGS-1210-28MP:5#
```

delete authen server_group

Purpose	To delete a user-defined authentication server host.
Syntax	**delete authen server_group <string 15>**
Description	The **delete authen server_ group** command deletes a user-defined authentication server group previously created on the Switch.

Parameters	*<string 15>* –Specifies the authentication server group name to be deleted.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete a user-defined rd1 authentication server group:

```
DGS-1210-28MP:5# delete authen server_group dlinkgroup
Command: delete authen server_group dlinkgroup

Success.
DGS-1210-28MP:5#
```

show authen server_group

Purpose	To view a user-defined authentication server group.
Syntax	**show authen server_group {<string 15>}**
Description	The **show authen server_ group** command displays user-defined authentication server groups previously created on the Switch. The following parameters are displayed: Group Name – The name of the server group. IP Address – The IP address of the authentication server group. Protocol – The protocol used by the server group.
Parameters	None.
Restrictions	None.

Example usage:

To view authenticaion server hosts currently set on the Switch:

```
DGS-1210-28MP:5#  show authen server_group
Command: show authen server_group

Group Name  : radius
      IP Address  : 10.90.90.97
      Protocol      : radius



Group Name  : dlinkgroup

Total Entries: 2
DGS-1210-28MP:5#
```

enable admin

Purpose	To promote user level privileges to administrator level privileges.
Syntax	**enable admin**
Description	The **enable admin** command enables a user to be granted administrative privileges on to the Switch. After logging on to the

	Switch, users have only 'user' level privileges. To gain access to administrator level privileges, the user may enter this command. The system then prompts for an authentication password. Possible authentication methods for this function include TACACS, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (none). Because TACACS does not support the enable function, the user must create a special account on the server host which has the username 'enable', and a password configured by the administrator that will support the 'enable' function. This function becomes inoperable when the authentication policy is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable administrator privileges on the Switch:

```
DGS-1210-28MP:5# enable admin
Command: enable admin

Success.
DGS-1210-28MP:5#
```

34

POWER SAVING COMMANDS

The Power Saving commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config power_saving mode	[hibernation | led | length_detection | port] [enable | disable]
config power_saving	[hibernation | led [all | <portlist>] | port [all | <portlist >]] [add | delete] time_range1 <range_name 20> time_range2 <range_name 20> {clear_time_range}
show power_saving	{hibernation | led | length_detection | port}

Each command is listed in detail, as follows:

config power_saving mode

Purpose	To configure the power saving mode on the switch.
Syntax	**config power_saving mode [hibernation | led | length_detection | port] [enable | disable]**
Description	The **config power_saving mode** command is used to configure the power saving mode on the switch.
Parameters	*hibernation* – Configure the hibernation state to enable or disable. The default value is disabled. *led* – Configure the led state to enable or disable. The default value is disabled. *length_detection* – Configure the length detection state to enable or disable. The default value is disabled. *port* – Configure ports state to be enabled or disabled. *[enable | disable]* – Enable or disable the power saving feature.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure the power saving mode on the switch:

```
DGS-1210-28MP:5#  config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable


Success.
DGS-1210-28MP:5#
```

config power_saving

Purpose	To configure the power saving on the switch.
Syntax	**config power_saving [hibernation | led [all | <portlist >] | port**

	[all | <portlist>]] [add | delete] time_range1 <range_name 20> time_range2 <range_name 20> {clear_time_range}
Description	The **config power_saving** command is used to configure the power saving on the switch.
Parameters	hibernation – Configure the hibernation. *led [all | <portlist >]* – Configure the ports for led. *port* – Configure ports. *[add | delete]* – Add or delete time range for power saving mode. *time_range1 <range_name 20>* – Specifies the time range 1 to be configured. *time_range2 <range_name 20>* – Specifies the time range 2 to be configured. *{clear_time_range}* – Clear the time range setting for power saving on the Switch.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure the power saving on the switch:

```
DGS-1210-28MP:5#  config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable

Success.
DGS-1210-28MP:5#
```

show power_saving

Purpose	To display power saving information on the switch.
Syntax	**show power_saving {hibernation | led | length_detection | port}**
Description	The **show power_saving** is used to display power saving information.
Parameters	hibernation – Display the hibernation state. *led* –Display the led state. *length_detection* –Display the length detection state. *port* –Display ports state.
Restrictions	None.

Example usage:

To display power saving information on the switch:

```
DGS-1210-28MP:5#  show power_saving length_detection
Command: show power_saving length_detection

Length Detection State   : Enabled
DGS-1210-28MP:5#
```

35

LLDP COMMANDS

The LLDP commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
enable lldp	
disable lldp	
config lldp message_tx_interval	<sec 5-32768>
config lldp message_tx_hold_multiplier	<int 2-10>
config lldp reinit_delay	<sec >
config lldp tx_delay	<sec 1-8192>
show lldp	
show lldp ports	{<portlist >}
show lldp local_ports	{<portlist >} {mode[brief | normal | detailed]}
show lldp remote_ports	{<portlist >} {mode[brief | normal | detailed]}
config lldp ports	[<portlist > | all] notification [enable | disable]
config lldp ports	[<portlist > | all] admin_status [tx_only | rx_only | tx_and_rx | disable]
config lldp ports	[<portlist >|all] mgt_addr [ipv4 <ipaddr>| ipv6 <ipv6addr>] [enable | disable]
config lldp ports	[<portlist >|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]
config lldp ports	[<portlist >|all] dot3_tlvs [all | link aggregation | mac_phy_configuration_status | maximum_frame_size] [enable | disable]
config lldp ports	[<portlist >|all] dot1_tlv_pvid [disable | enable]
config lldp ports	[<portlist >|all] dot1_tlv_protocol_identity eapol [disable | enable]
config lldp ports	[<portlist >|all] dot1_tlv_vlan_name [vlan [<vlan_name 20> | all] | vlanid <vidlist 1-4094>] [disable | enable]
show lldp mgt_addr	{ipv4 <ipaddr> | ipv6 <ipv6addr>}
show lldp statistics	{ports <portlist >}
show lldp power_pse_tlv	

Each command is listed in detail, as follows:

enable lldp	
Purpose	To enable LLDP on the switch.

Syntax	**enable lldp**
Description	The **enable lldp** command enables the *Link Layer Discovery Protocol* (LLDP) on the switch.
Parameters	None
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To enable LLDP on the switch:

```
DGS-1210-28MP:5# enable lldp
Command: enable lldp

Success.
DGS-1210-28MP:5#
```

disable lldp

Purpose	To disable LLDP on the switch.
Syntax	**disable lldp**
Description	The **disable lldp** command disables the *Link Discovery Protocol* (LLDP) on the switch.
Parameters	None
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To disable LLDP on the switch:

```
DGS-1210-28MP:5# disable lldp
Command: disable lldp

Success.
DGS-1210-28MP:5#
```

config lldp message_tx_interval

Purpose	To define the lldp message tx interval
Syntax	**config lldp message_tx_interval <sec 5-32768>**
Description	The **config lldp message_tx_interval** defines the lldp message interval of the incoming messages.
Parameters	*<sec 5-32768>* – Defines the message interval time. The range is between 5 and 32768.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure LLDP message tx interval on the switch:

```
DGS-1210-28MP:5# config lldp message_tx_interval 10
Command: config lldp message_tx_interval 10

Success.
DGS-1210-28MP:5#
```

config lldp message_tx_hold_multiplier

Purpose	To define the lldp hold-multiplier on the switch.
Syntax	**config lldp message_tx_hold_multiplier <int 2-10>**
Description	The **config lldp message_tx_hold_multiplier** command specifies the amount of time the receiving device should hold a *Link Layer Discovery Protocol* (LLDP) packet before discarding it.
Parameters	*message_tx_hold_multiplier (int 2-10)* – Specifies the hold time to be sent in the LLDP update packets as a multiple of the timer value. (Range: 2-10). The default configuration is 4.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP Message tx hold multiplier settings:

```
DGS-1210-28MP:5# config lldp message_tx_hold_multiplier 2
Command: config lldp message_tx_hold_multiplier 2

Success.
DGS-1210-28MP:5#
```

config lldp reinit_delay

Purpose	To define the lldp reinint–delay on the switch.
Syntax	**config lldp reinit_delay <sec >**
Description	The **lldp reinit_delay** *seconds* command specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.
Parameters	*<sec >* – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 10 seconds. The default configuration is 2 seconds.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure LLDP reinit delay:

```
DGS-1210-28MP:5# config lldp reinit_delay 1
Command: config lldp reinit_delay 1


Success.
DGS-1210-28MP:5#
```

config lldp tx_delay

Purpose	To configure the lldp tx_delay on the switch.

Syntax	**config lldp tx_delay <sec 1-8192>**
Description	The **config lldp tx_delay** command specifies the delay between successive LLDP frame transmissions initiated by value/status changes in the LLDP local systems MIB, use the **lldp tx_delay** command in global configuration mode.
Parameters	*<sec 1-8192>* – Specifies the minimum time in seconds an LLDP port will wait before reinitializing LLDP transmission. The range is 1 – 8192 seconds. The default configuration is 2 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP tx delay:

```
DGS-1210-28MP:5# config lldp tx_delay 1
Command: config lldp tx_delay 1

Success.
DGS-1210-28MP:5#
```

show lldp

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) on the switch.
Syntax	**show lldp**
Description	The **show lldp** displays the LLDP configuration on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show LLDP settings:

```
DGS-1210-28MP:5# show lldp
Command: show lldp

LLDP System Information
----------------------------------------
Chassis ID Subtype        : MAC Address
Chassis ID              : EC-AD-E0-62-AF-A0
System Name             :
System Description      : DGS-1210-28MP 2.00.005
System Capabilities     : bridge

LLDP Configurations
----------------------------------------
LLDP Status             : Disabled
Message Tx Interval     : 30
Message Tx Hold Multiplier  : 4
ReInit Delay            : 2
Tx Delay                : 2
DGS-1210-28MP:5#
```

show lldp ports

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) ports

	configuration on the switch.
Syntax	**show lldp ports {<portlist >}**
Description	The **show lldp ports** command displays the information regarding the ports.
Parameters	*<portlist* > − A port or range of ports to be displayed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To show the information for port 1:

```
DGS-1210-28MP:5#  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 Capabilitiess                      Disabled
   Enabled Management Address
     <None>
   Port VLAN ID                              Disabled
   Enabled VLAN Name
     <None>
   Enabled Protocol_Identity
     <None>
   MAC/PHY Configuration/Status              Disabled
   Maximum Frame Size                        Disabled

DGS-1210-28MP:5#
```

show lldp local_ports

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) configuration that is advertised from a specific port.
Syntax	**show lldp local_ports {<portlist >} {mode[brief | normal | detailed]}**
Description	The **show lldp local_ports** command displays the configuration that is advertised from a specific port.
Parameters	*<portlist* > − A port or range of ports to be displayed. *{mode[brief* | *normal* | *detailed]}* − defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To show the local port information for port 1 with mode brief:

```
DGS-1210-28MP:5#  show lldp local_ports 1 mode brief
Command: show lldp local_ports 1 mode brief

Port ID : 1
----------------------------------------
Port Id Subtype                : Interface Alias
Port Id                        : Fa0/1
Port Description               :

DGS-1210-28MP:5#
```

show lldp remote_ports

Purpose	To display information regarding the neighboring devices discovered using LLDP.
Syntax	**show lldp remote_ports {<portlist >} {mode[brief | normal | detailed]}**
Description	The **show lldp remote_ports command** displays the information regarding neighboring devices.
Parameters	*<portlist* > − A port or range of ports to be displayed. *[mode[brief* | *normal* | *detailed]}* − defines which mode of information want to be displayed, brief, normal or detailed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To show the information for remote ports:

```
DGS-1210-28MP:5# show lldp remote_ports 1 mode normal
Command: show lldp remote_ports 1 mode normal

Port ID : 1
------------------------------------------------------------------------------
Remote Entities Count : 0
   (NONE)

DGS-1210-28MP:5#
```

config lldp ports

Purpose	To enable LLDP notification on a port or ports.
Syntax	**config lldp ports [<portlist > | all] notification [enable | disable]**
Description	The **config lldp ports** notification command defines lldp notification per port on the switch.
Parameters	*ports [<portlist* > | *all]* – Specify a port or ports to be configured. *notification [enable* | *disable]*– defines is notification is enabled or disabled.
Restrictions	Only Administrator or operator-evel users can issue this command.

Example usage:

To configure LLDP notification:

```
DGS-1210-28MP:5# config lldp ports 1-3 notification enable
Command: config lldp ports 1-3 notification enable

Success.
DGS-1210-28MP:5#
```

config lldp ports	
Purpose	To define LLDP admin status on a port or ports.
Syntax	**config lldp ports [<portlist > | all] admin_status [tx_only | rx_only | tx_and_rx | disable]**
Description	The **config lldp ports** admin status command defines lldp admin status per port on the switch.
Parameters	*[<portlist> | all]* – Specify a port or ports to be configured. *Admin status* – defines admin status of ports on the switch Tx- Tx only Rx – Rx only Both – Tx and RX Disable – admin status disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP admin status

```
DGS-1210-28MP:5# config lldp ports 2 admin_status disable
Command: config lldp ports 2 admin_status disable

Success.
DGS-1210-28MP:5#
```

config lldp ports	
Purpose	To define LLDP management address advertisement on a port or ports.
Syntax	**config lldp ports [<portlist >|all] mgt_addr [ipv4 <ipaddr>| ipv6 <ipv6addr>] [enable | disable]**
Description	The **config lldp ports** mgt_addr command defines if lldp will advertise the switch's IP address the command is per port on the switch.
Parameters	*[<portlist* > | *all]* – Specify a port or ports to be configured. *mgt_addr [ipv4 <ipaddr>* | *ipv6 <ipv6addr>]* – defines wether the management address (IPv4 or IPv6 address) advertisement will be enabled or disabled
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP management address advertisement

```
DGS-1210-28MP:5# config lldp ports 1 mgt_addr ipv4 100.1.1.2 enabled
Command: config lldp ports 1 mgt_addr ipv4 100.1.1.2 enabled

Success.
DGS-1210-28MP:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist >|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]**
Description	The **config lldp ports** basic TLVs command defines if lldp will advertise the switch's basic TLVs the command is per port on the switch.
Parameters	*[<portlist* > | *all]* – Specify a port or ports to be configured. *Basic TLVs:* *all* – Advertisement of all the basic TLVs *port description* – Advertisement of *Port description* *system name* – Advertisement of *system name* *system description* – Advertisement of *System description* *system capabilities* – Advertisement of system capabilities
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP Basis TLVs

```
DGS-1210-28MP:5# config lldp ports 1 basic_tlvs all enable
Command: config lldp ports 1 basic_tlvs all enable

Success.
DGS-1210-28MP:5#
```

config lldp ports

Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist>|all] dot3_tlvs [all | link aggregation | mac_phy_configuration_status | maximum_frame_size] [enable | disable]**
Description	The **config lldp ports** dot3 TLVs command defines if lldp will advertise the mac_phy_configuration_status the command is per port on the switch.
Parameters	*[<portlist* > | *all]* – Specify a port or ports to be configured. *dot3_tlvs* – defines if the advertisement is enabled or disabled. The possible values are: link_aggregation, mac_phy_configuration_status, maximum_frame_size or all.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP mac_phy_configuration status:

```
DGS-1210-28MP:5# config lldp ports 2 dot3_tlvs mac_phy_configuration_status
enable
Command: config lldp ports 2 dot3_tlvsmac_phy_configuration_status enable

Success.
DGS-1210-28MP:5#
```

config lldp ports	
Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist >|all] dot1_tlv_pvid [disable | enable]**
Description	The **config lldp ports** dot1 TLVs command defines if lldp will advertise the mac_phy_configuration_status the command is per port on the switch.
Parameters	*[<portlist* > | *all]* – Specify a port or ports to be configured. *[enable* | *disable]* - Defines if the advertisement is enabled or disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP TLV PVID:

```
DGS-1210-28MP:5# config lldp ports all dot1_tlv_pvid disable
Command: config lldp ports all dot1_tlv_pvid disable

Success.
DGS-1210-28MP:5#
```

config lldp ports	
Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist >|all] dot1_tlv_protocol_identity eapol [disable | enable]**
Description	The **config lldp ports** dot1 TLVs command defines if lldp will advertise the mac_phy_configuration_status the command is per port on the switch.
Parameters	*[<portlist* > | *all]* – Specify a port or ports to be configured. *dot1_tlv_protocol_identity* − Defines if the advertisement is enabled or disabled. The possible value is eapol.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP ports configuration status:

```
DGS-1210-28MP:5# config lldp ports all dot1_tlv_protocol_identity eapol enable
Command: config lldp ports all dot1_tlv_protocol_identity eapol enable

Success.
DGS-1210-28MP:5#
```

config lldp ports	
Purpose	To define LLDP management basic TLVs advertisement on a port or ports.
Syntax	**config lldp ports [<portlist >|all] dot1_tlv_vlan_name [vlan [<vlan_name 20> | all] | vlanid <vidlist 1-4094>] [disable | enable]**

Description	The **config lldp ports** dot1 TLVs command defines lldp admin status per port on the switch.
Parameters	*[<portlist >* | *all]* – Specify a port or ports to be configured. *vlan [<vlan_name 20>* | *all]* –The name of the VLAN to be configured. *dot1_tlv_vlan_name* − Defines if the advertisement is enabled or disabled. *vlanid <vidlist 1-4094>* –The vid of the VLAN to be configured.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP mac_phy_configuration status:

```
DGS-1210-28MP:5# config lldp ports all dot1_tlv_vlan_name vlanid 1 disable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1 disable

Success.
DGS-1210-28MP:5#
```

show lldp mgt_addr

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) configuration that is advertised from a specific port.
Syntax	**show lldp mgt_addr {ipv4 <ipaddr> | ipv6 <ipv6addr>}**
Description	The **show lldp mgt_addr** command displays the information regarding the IPv4 or IPv6 address.
Parameters	*ipv4 <ipaddr>* | *ipv6 <ipv6addr>* **–** Specifies the lldp IPv4 or IPv6 address to be displayed.
Restrictions	None.

Example usage:

To show the LLDP management address advertisement:

```
DGS-1210-28MP:5# show lldp mgt_addr
Command: show lldp mgt_addr


Address : 1
----------------------------------------
Subtype                 : IPv4
Address                 : 10.90.90.90
IF Type                 : ifIndex
OID                     : 1.3.6.1.2.1.2.2.1.1
Advertising Ports       : <NONE>

Total Address : 1
DGS-1210-28MP:5#
```

show lldp statistics

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) statistics for the specified ports.
Syntax	**show lldp statistics {ports <portlist >}**
Description	The **show lldp statistics** command displays the statistics of LLDP on the Switch.

Parameters	*{ports <portlist >* – Specifies the ports to be displayed.
Restrictions	None.

Example usage:

To show the LLDP statistics for port 3:

```
DGS-1210-28MP:5# show lldp statistics ports 3
Command: show lldp statistics ports 3

Port ID : 3
-----------------------------------------------
lldpStatsTxPortFramesTotal                : 0
lldpStatsRxPortFramesDiscardedTotal  : 0
lldpStatsRxPortFramesErrors               : 0
lldpStatsRxPortFramesTotal                : 0
lldpStatsRxPortTLVsDiscardedTotal     : 0
lldpStatsRxPortTLVsUnrecognizedTotal : 0
lldpStatsRxPortAgeoutsTotal               : 0

DGS-1210-28MP:5#
```

show lldp power_pse_tlv

Purpose	To display the *Link Layer Discovery Protocol* (LLDP) powers.
Syntax	**show lldp power_pse_tlv**
Description	The **show lldp power_pse_tlv** command displays the power of LLDP on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the LLDP power PSE status:

```
DGS-1210-28MP:5# show lldp power_pse_tlv
Command: show lldp power_pse_tlv


Port        State
-------------------------------------
1           Disable
2           Disable
3           Disable
4           Disable
DGS-1210-28MP:5#
```

36

TRAFFIC SEGMENTATION COMMANDS

The Traffic Segmentation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config traffic_segmentation	<portlist > forward_list [null | <portlist >]
show traffic_ segmentation	{<portlist >}

Each command is listed in detail, as follows:

config traffic_segmentation

Purpose	To configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation <portlist > forward_list [null | <portlist >]**
Description	The **config traffic_segmentation** command configures traffic segmentation on the Switch.
Parameters	*<portlist* > – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed. *forward_list* – Specifies a port or a port channel to receive forwarded frames from the source ports specified in the portlist, above.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure ports 1~3 to be able to forward frames to port 5:

```
DGS-1210-28MP:5# config traffic_segmentation 1-3 forward_list 5
Command: config traffic_segmentation 1-3 forward_list 5

Success.
DGS-1210-28MP:5#
```

show traffic_segmentation

Purpose	To display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation {<portlist >}**
Description	The **show traffic_segmentation** command displays the current traffic segmentation configuration on the Switch.
Parameters	*<portlist* > – A port or a port channel for which the current traffic segmentation configuration on the Switch is to be displayed.
Restrictions	None.

Example usage:

To display the current traffic segmentation configuration on the Switch:

```
DGS-1210-28MP:5#  show traffic_segmentation
Command: show traffic_segmentation


Traffic Segmentation Table

Port Forward Portlist
------ ----------------------
1
2
3
4
5
6
7
8
9
10

DGS-1210-28MP:5#
```

37

ETHERNET OAM COMMANDS

Ethernet OAM (Operations, Administration, and Maintenance) is a data link layer protocol which provides network administrators the ability to monitor the health of the network and quickly determine the location of failing links or fault conditions on point-to-point and emulated point-to-point Ethernet link. The Ethernet OAM commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config ethernet_oam ports (mode)	[all | <portlist >] mode [active | passive]
config ethernet_oam ports (state)	[all | <portlist >] state [enable | disable]
config ethernet_oam ports (link monitor error symbol)	[all | <portlist >] link_monitor error_symbol {threshold <integer 1-4294967295> | window < integer 1000-60000> | notify_state [enable | disable]}
config ethernet_oam ports (link monitor error frame)	[all | <portlist >] link_monitor error_frame {threshold <integer> | window < integer 1000-60000> | notify_state [enable | disable]}
config ethernet_oam ports (link monitor error frame seconds)	[all | <portlist >] link_monitor error_frame_seconds {threshold < integer 1-4294967295> | window < integer 1000-60000> | notify_state [enable | disable]}
config ethernet_oam ports (link monitor error frame period)	[all | <portlist >] link_monitor error_frame_period {threshold < integer 1-4294967295> | window < integer 148810-100000000> | notify_state [enable | disable]}
config ethernet_oam ports (remote loopback)	[all | <portlist >] remote_loopback [start | stop]
config ethernet_oam ports (received remote loopback)	[all | <portlist >] received_remote_loopback [process | ignore]
show ethernet_oam ports (status)	[all | <portlist >] status
show ethernet_oam ports (configuration)	[all | <portlist >] configuration
show ethernet_oam ports (statistics)	[all | <portlist >] statistics
show ethernet_oam ports (event log)	[all | <portlist >] event_log {index <value_list}
clear ethernet_oam ports	[all | <portlist >] [event_log| statistics]

Each command is listed in detail, as follows:

config ethernet_oam ports (mode)

Purpose	Used to configure Ethernet OAM mode for ports.
Syntax	**config ethernet_oam ports [all | <portlist >] mode [active | passive]**
Description	The **config ethernet_oam ports** command is used to configure Ethernet OAM for ports to operate in active or passive mode.
Parameters	The command is used to configure Ethernet OAM for ports to operate in active or passive mode. Port configured in *active* mode: (1) Initiate the exchange of Information OAMPDUs as defined by the discovery state diagram. (2) Active port is permitted to send any OAMPDU while connected to a remote OAM peer entity in active mode. (3) Active port operates in a limited respect if the remote OAM entity is operating in passive mode. (4) Active port should not respond to OAM remote loopback commands and variable requests from a passive peer. Port configured in *passive* mode: (1) Do not initiate the discovery process (2) React to the initiation of the Discovery process by the remote. This eliminates the possibility of passive-to-passive links. (3) Shall not send Variable request or loopback Control OAMPDUs" for describe the active and passive mode.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure port 1 OAM mode to passive:

```
DGS-1210-28MP:5#  config ethernet_oam ports 1 mode passive
Command: config ethernet_oam ports 1 mode passive

Success.
DGS-1210-28MP:5#
```

config ethernet_oam ports (state)

Purpose	Used to enable or disable Ethernet OAM per port.
Syntax	**config ethernet_oam ports [all | <portlist >] state [enable | disable]**
Description	The **config ethernet_oam ports** command is used to enable or disable Ethernet OAM function on a per port basis. Enabling OAM initiates OAM discovery on a port. When OAM is enabled on a port in active mode, that port will initiate discovery; if the port is not OAM enabled, the port will not participate in the discovery process.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *state [enable | disable]* – Specify to enable or disable the OAM function for the listed ports. The default state is disabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable Ethernet OAM on port 1:

```
DGS-1210-28MP:5#  config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.
DGS-1210-28MP:5#
```

config ethernet_oam ports (link monitor error symbol)

Purpose	Used to configure Ethernet OAM link monitoring symbol error configuration for ports.
Syntax	**config ethernet_oam ports [all | <portlist >] link_monitor error_symbol {threshold <integer> | window < integer 1000-60000> | notify_state [enable | disable]}**
Description	The **config ethernet_oam ports** command is used to configure Ethernet OAM link monitoring symbol error for ports. 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.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – Specify the number of symbol errors in the period that must be equal to or greater than in order for the event to be generated. The default value of the threshold is 1 symbol error. *window <integer 1000-60000>* –The range is 1000 to 60000 ms. The default value is 1000ms. *notify_state [enable | disable]* – Specify to enable or disable event notification. The default state is enabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-1210-28MP:5#  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-1210-28MP:5#
```

config ethernet_oam ports (link monitor error frame)	
Purpose	Used to configure Ethernet OAM link monitoring error frame configuration for ports.
Syntax	**config ethernet_oam ports [all | <portlist >] link_monitor error_frame {threshold <integer> | window < integer 1000-60000> | notify_state [enable | disable]}**
Description	The **config ethernet_oam ports** command is used to configure Ethernet OAM link monitoring error frames for ports. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counts of 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.
Parameters	*[all* | *<portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – Specify the number of frame errors in the period that must be equal to or greater than in order for the event to be generated. The default value is 1 frame error. *window <integer 1000-60000>* –The range is 1000 to 60000 ms. The default value is 1000ms. *notify_state [enable* | *disable]* – Specify to enable or disable event notification. The default state is enabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the error symbol threshold to 2 and period to 1000ms for port 1:

```
DGS-1210-28MP:5#  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-1210-28MP:5#
```

config ethernet_oam ports (link monitor error frame seconds)	
Purpose	Used to configure Ethernet OAM link monitoring error frame seconds configuration for ports.
Syntax	**config ethernet_oam ports [all | <portlist >] link_monitor error_frame_seconds {threshold < integer> | window < integer 1000-60000> | notify_state [enable | disable]}**
Description	The **config ethernet_oam ports** command is used to configure Ethernet OAM link monitoring error frame seconds for ports. An error frame second is one second interval wherein at least one frame error was detected. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counts of the number of frame errors as well as the number of coding symbol errors. When the number of error frame seconds is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame seconds summary event to notify the remote OAM peer.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – Specify the number of error frame seconds in the period that must be equal to or greater than in order for the event to be generated. The default value is 1 frame error. *window <integer 1000-60000>* –Specify the period of error frame seconds summary event. The range is 1000ms-60000ms and the default value is 60000 ms. *notify_state [enable | disable]* – Specify to enable or disable event notification. The default state is enabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the error frame seconds threshold to 2 and period to 10000 ms for port 1:

```
DGS-1210-28MP:5#  config ethernet_oam ports 1 link_monitor error_frame threshold 2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame threshold 2 window 10000 notify_state enable


Success.
DGS-1210-28MP:5#
```

config ethernet_oam ports (link monitor error frame period)

Purpose	Used to configure Ethernet OAM link monitoring error frame period for ports.
Syntax	**config ethernet_oam ports [all | <portlist >] link_monitor error_frame_period {threshold < integer> | window < integer 148810-100000000> | notify_state [enable | disable]}**
Description	The **config ethernet_oam ports** command is used to configure ports Ethernet OAM link monitoring error frame period. 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 error frames is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame period event to notify the remote OAM peer.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured. *threshold <integer>* – Specify the number of error frames in the period that must be equal to or greater than in order for the event to be generated. The default value of threshold is 1 error frame. *window <integer 148810-100000000>* – Specify the period of error frame period event. The period is specified by a number of received frames. The default value is 148810. *notify_state [enable | disable]* – Specify to enable or disable event notification. The default state is enabled.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the error frame threshold to 10 and period to 1000000 for port 1:

```
DGS-1210-28MP:5#  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-1210-28MP:5#
```

config ethernet_oam ports (remote loopback)

Purpose	Used to start or stop Ethernet OAM remote loopback mode for the remote peer of the port.
Syntax	**config ethernet_oam ports [all | <portlist >] remote_loopback [start | stop]**
Description	The **config ethernet_oam ports** command is used to start or stop the remote peer to enter Ethernet OAM remote loopback mode. To start the remote peer to enter remote loopback mode, the port must be in active mode and the OAM connection established. If the local client is already in remote loopback mode, then the command cannot be applied.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to be configured.

	remote_loopback [start | *stop]* – If start is specified, a request is sent to the remote peer to change to remote loopback mode. If stop is specified, a request is sent to the remote peer to change to normal operation mode.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To start remote loopback on port 1 of unit 1:

```
DGS-1210-28MP:5# config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start

Success.
DGS-1210-28MP:5#
```

config ethernet_oam ports (received remote loopback)

Purpose	Used to configure the method to process the received Ethernet OAM remote loopback command.
Syntax	**config ethernet_oam ports [all | <portlist >] received_remote_loopback [process | ignore]**
Description	The **config ethernet_oam ports** command is used to configure the client to process or to ignore a received Ethernet OAM remote loopback command. In remote loopback mode, user traffic is not forwarded on the port. If ignore is specified for received_remote_loopback, the specified port will ignore all requests to transition to remote loopback mode and prevent the Switch from entering remote loopback mode, thus it continues to process user traffic regardless.
Parameters	*[all* | *<portlist >]* – Specifies a range of ports or all ports to be configured. *received_remote_loopback [process* | *ignore]* – Specify whether to process or ignore the received Ethernet OAM remote loopback command. The default method is “ignore”.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the method of processing the received remote loopback command as “process” on port 1:

```
DGS-1210-28MP:5# config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.
DGS-1210-28MP:5#
```

show ethernet_oam ports (status)

Purpose	Used to display primary controls and status information for Ethernet OAM per port.
Syntax	**show ethernet_oam ports [all | <portlist >] status**
Description	The **show ethernet_oam ports** command is used to show primary controls and status information for Ethernet OAM on specified ports. The 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 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. (7) **Loopback Status**: The current status of the loopback function of the port: ☐ **No Loopback** – The local and remote ports are not in loopback

	mode. ☐ **Initiating Loopback** – The local port has sent the start remote loopback request to the peer and is waiting for response. ☐ **Remote Loopback** – This indicates that both the local and remote ports entered the loopback mode. Any non-OAM packet received in the local port will be dropped. ☐ **Local Loopback** – This indicates that both the local and remote ports entered the loopback mode. The local port is doing the loopback. Any non-OAM packets received on the port will be sent back to the same port. ☐ **Terminate Loopback** - The port is stopping loopback on the port.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to display status.
Restrictions	None.

Example usage:

To show OAM control and status information on port 3:

```
DGS-1210-28MP:5#  show ethernet_oam ports 3 status
Command: show ethernet_oam ports 3 status


Port 3
Local Client
---------------------------------------------------------------
OAM                          : Disabled
Mode                         : Passive
Max OAMPDU                   : 1518
Remote Loopback              : Support
Unidirection                 : Not Supported
Link Monitoring              : Support
Variable Request             : Support
PDU Revision                 : 0
Operation Status             : Disabled
Loopback Status              : No Loopback

Remote Client
---------------------------------------------------------------
Mode                         : Unknown
MAC Address                  : 00:00:00:00:00:00
Vendor (OUI)                 : 00:00:00
```

show ethernet_oam ports (configuration)

Purpose	Used to display Ethernet OAM configuration per port.
Syntax	**show ethernet_oam ports [all | <portlist >] configuration**
Description	The **show ethernet_oam ports** command is used to view Ethernet OAM configurations for ports.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to display status.

Restrictions	None.

Example usage:

To show Ethernet OAM configuration on port 3:

```
DGS-1210-28MP:5#  show ethernet_oam ports 3 configuration
Command: show ethernet_oam ports 3 configuration


Port 3
---------------------------------------------------------------
OAM                                 : Disabled
Mode                                : Passive
Critical Event                      : Enabled
Remote Loopback OAMPDU              : Not Processed

Symbol Error
Notify State                        : Enabled
Window                              : 1000
Threshold                           : 23

Frame Error
Notify State                        : Enabled
Window                              : 1000
Threshold                           : 1

Frame Period Error
Notify State                        : Enabled
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

show ethernet_oam ports (statistics)

Purpose	Used to display Ethernet OAM statistics for ports.
Syntax	**show ethernet_oam ports [all | <portlist >] statistics**
Description	The **show ethernet_oam ports** command is used to display Ethernet OAM ports statistics information.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to display status.
Restrictions	None.

Example usage:

To show Ethernet OAM statistics on port 2:

```
DGS-1210-28MP:5#  show ethernet_oam ports 2 statistics
Command: show ethernet_oam ports 2 statistics


Port 2
------------------------------------------------------------------------
  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-1210-28MP:5#
```

show ethernet_oam ports (event log)

Purpose	Used to display Ethernet OAM event log.
Syntax	**show ethernet_oam ports [all | <portlist >] event_log {index <value_list>}**
Description	The **show ethernet_oam ports** command is used to view ports Ethernet OAM event log information. The Switch can buffer 1000 event logs. The event log is different from sys-log. It provides more detailed information than sys-log. Each OAM event will be recorded in both OAM event log and syslog. Specify an index to show a range of events.
Parameters	*[all | <portlist >]* – Specifies a range of ports or all ports to display status. *index <value_list>* – Specifies an index range to display.
Restrictions	None.

Example usage:

To show Ethernet OAM event log on port 1:

```
DGS-1210-28MP:5#  show ethernet_oam ports 1 event_log index 2
Command: show ethernet_oam ports 1 event_log index 2


Port 1
------------------------------------------------------------
Event Listing:
Index  Type              Location   Time Stamp          Value      Window
  Threshold  Accumulated errors
-----  -------------------  ---------- -------------------- ---------- --------
-- ---------- --------------------
DGS-1210-28MP:5#
```

clear ethernet_oam ports

Purpose	Used to clear Ethernet OAM port statistics or event log.
Syntax	**clear ethernet_oam ports [all | <portlist >] [event_log| statistics]**
Description	The **clear ethernet_oam ports** command is used to clear Ethernet OAM ports statistics or event log information.
Parameters	*[all* | *<portlist>]* – Specifies a range of ports or all ports to clear OAM statistics or event log. *[event_log* | *statistics]*> – Specifies an index range to display.
Restrictions	None.

Example usage:

To clear port 1 OAM statistics:

```
DGS-1210-28MP:5#  clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.
DGS-1210-28MP:5#
```

38

SAFEGUARD COMMANDS

The Safeguard commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config safeguard_engine	state [enable | disable]
show safeguard_engine	

Each command is listed in detail, as follows:

config safeguard_engine	
Purpose	To define the safeguard engine on the switch.
Syntax	**config safeguard_engine state [enable | disable]**
Description	To define the safeguard_engine on the switch. Safeguard is a protection mechanism that limits packets forwarded to CPU, for exmplae: ARP, ICMP, IGMP, etc,
Parameters	*state [enable* | *disable]* – enable and disable Safeguard engine on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the safeguard engine on the switch:

```
DGS-1210-28MP:5# config safeguard_engine state enable
Command: config safeguard_engine state enable

Success.
DGS-1210-28MP:5#
```

show safeguard_engine	
Purpose	To show the safeguard engine status on the switch.
Syntax	**show safeguard_engine**
Description	To show the safeguard engine on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the safeguard engine status on the switch:

```
DGS-1210-28MP:5#  show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State        :   Enable

DGS-1210-28MP:5#
```

39

ACCESS CONTROL LIST COMMANDS

The Access Control List commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create access_profile	[ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip { 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} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> } | protocol_id_mask <0x0-0xff>]} | packet_content_mask {offset1 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff> | offset2 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff>| offset3 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff>| offset4 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff>} | ipv6 { class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp { type | code }]} profile_id <value 1-50>]
config access_profile	profile_id [value <1-50>] [add access_id [auto_assign | <value 1-128>] [ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x05dd-0xffff> } | ip {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>]} | packet_content [offset1 <hex 0x0-0xffffffff> | offset2 <hex 0x0-0xffffffff> | offset3 <hex 0x0-0xffffffff> | offset4 <hex 0x0-0xffffffff>] | ipv6 [class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> | tcp [src_port < value 0-65535> | dst_port < value 0-65535>] | udp [src_port < value 0-65535> | dst_port < value 0-65535>] | icmp [type<value 0-255> | code <value 0-255>]] [port [<portlist> | all] [permit {replace_priority_with <value 0-7> | replace_dscp_with <value 0-63> | rx_rate {no_limit | <value 64-1024000>}} | mirror | deny]] | delete access_id <value 1-128>]
delete access_profile	[all | profile_id <value 1-50>]
show access_profile	{profile_id <value 1-50>}
create cpu_access_profile	[ethernet {vlan | source_mac <macmask> | Destination_mac <macmask> | 802.1p | ethernet_type} | ip {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} | udp {src_port_mask <hex (0x0-0xffff)> | dst_port_mask <hex (0x0-0xffff)>} | protocol_id_mask <hex (0x0-0xff)>]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}] profile_id <value 1-3>
config cpu_access_profile	[profile_id <value 1-3] [add access_id [auto_assign | <value 1-5>]] [ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {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>] | ipv6 {class | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>} [port [<portlist> | all]

Command	Parameter
	[permit | deny]] delete access_id <value 1-5>]
delete cpu access_profile	profile_id <value 1-3>
show cpu access_profile	{profile_id <value 1-3>}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
config flow_meter profile_id	<value 1-50> access_id <value 1-250> [delete | rate <value 64-1024000>] rate_exceed [drop_packet | remark_dscp <value 0-63>]
show flow_meter	{profile_id <value 1-50> | access_id <value 1-250>}

Each command is listed in detail, as follows:

create access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip { 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} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> } | protocol_id_mask <0x0-0xff>]} | packet_content_mask {offset1 [l2 | l3 | l4] <value 0-31> <hex (0x0-0xffff)> | offset2 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff>| offset3 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff>| offset4 [l2 | l3 | l4] <value 0-31> <hex 0x0-0xffff>} | ipv6 { class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask> | [tcp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | icmp { type | code }]} profile_id <value 1-50>]**
Description	The **create access_profile** command creates a profile for packets that may be accepted or denied by the Switch by examining the Ethernet part of the packet header. Specific values for rules pertaining to the Ethernet part of the packet header may be defined by configuring the **config access_profile** command for Ethernet, as stated below.
Parameters	*ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies that the Switch examine the VLAN part of each packet header. • *source_mac* <*macmask*> – Specifies a MAC address mask for the source MAC address. This mask is entered in the following hexadecimal format: 000000000000-FFFFFFFFFFFF.

- *destination_mac <macmask>* – Specifies a MAC address mask for the destination MAC address in the following format: 000000000000-FFFFFFFFFFFF.
- *802.1p* – Specifies that the Switch examine the 802.1p priority value in the frame's header.
- *ethernet_type* – Specifies that the Switch examine the Ethernet type value in each frame's header.

ip - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following:

icmp – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place.

- *type* – Specifies that the Switch examines each frame's ICMP Type field.
- *code* – Specifies that the Switch examines each frame's ICMP Code field.

igmp – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place.

- *type* – Specifies that the Switch examine each frame's IGMP Type field.

tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.

- *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
- *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port.
- *flag_mask* – Specifies the appropriate flag_mask parameter.

udp – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place..

- *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port.
- *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port.

packet_content_mask – Specifies the frame content mask.

[offset1 | offset2 | offset3 | offset4] – Specifies the mask pattern offset of frame.

Ipv6 – Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following:

class – Examine the class field of the IPv6 header.

source_ipv6_mask <ipv6mask> – Specifies the IPv6 address mask for the source IP.

destination_ipv6_mask <ipv6mask> – Specifies the IPv6 address mask for the destination IP.

tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.

- *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
- *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port

	mask for the destination port. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.. • *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *type* – Specifies that the Switch examines each frame's ICMP Type field. • *code* – Specifies that the Switch examines each frame's ICMP Code field. *profile_id <value 1-50>* – Specifies an index number between 1 and 50 that identifies the access profile being created with this command. The maximum entries for profile ID is 6.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create an Ethernet access profile:

```
DGS-1210-28MP:5# create access_profile ethernet vlan 802.1p profile_id 1
Command: create access_profile ethernet vlan 802.1p profile_id 1

Success.
DGS-1210-28MP:5#
```

To create an IPv6 access profile:

```
DGS-1210-28MP:5# create access_profile ipv6 source_ipv6_mask
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff profile_id 1
Command: create access_profile ipv6 source_ipv6_mask ffff:ffff:ffff:ffff:ffff:ff
ff:ffff:ffff profile_id 1

Success.

DGS-1210-28MP:5#
```

config access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**config access_profile profile_id [value <1-50>] [add access_id [auto_assign | <value 1-128>] [ethernet {vlan <vlanid 1-4094> |**

	source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x05dd-0xffff> } | ip {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>]} | packet_content [offset1 <hex 0x0-0xffffffff> | offset2 <hex 0x0-0xffffffff> | offset3 <hex 0x0-0xffffffff> | offset4 <hex 0x0-0xffffffff>] | ipv6 [class <value 0-255> | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr> | tcp [src_port < value 0-65535> | dst_port < value 0-65535>] | udp [src_port < value 0-65535> | dst_port < value 0-65535>] | icmp [type<value 0-255> | code <value 0-255>]] [port [<portlist> | all] [permit {replace_priority_with <value 0-7> | replace_dscp_with <value 0-63> | rx_rate {no_limit | <value 64-1024000>}} | mirror | deny]] | delete access_id <value 1-128>]
Description	The **config access_profile ethernet** command defines the rules used by the Switch to either filter or forward packets based on the Ethernet part of each packet header.
Parameters	*profile_id <value 1-50>* – Specifies the access profile id to be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The lower the profile ID, the higher the priority the rule will be given. *[add | delete] access_id <value 1-128>* – Adds or deletes an additional rule to the above specified access profile. The value specifies the relative priority of the additional rule. Up to 65535 rules may be configured for the Ethernet access profile. • *auto_assign* – Configures the Switch to automatically assign a numerical value (between 1 and 128) for the rule being configured. *ethernet* – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following: • *vlan <vlanid 1-4094>* – Specifies that the access profile applies only to this previously created VLAN. • *source_mac <macaddr>* – Specifies that the access profile applies only to packets with this source MAC address. MAC address entries may be made in the following format: 000000000000-FFFFFFFFFFFF. • *destination_mac <macaddr>* – Specifies that the access profile applies only to packets with this destination MAC address. MAC address entries may be made in the following format: 000000000000-FFFFFFFFFFFF • *802.1p <value 0-7>* – Specifies that the access profile applies only to packets with this 802.1p priority value. • *ethernet_type <hex 0x05dd-0xffff>* – Specifies that the access profile applies only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header. *ports <portlist>* - The access profile for Ethernet may be defined for each port on the Switch. • *mirror* – Specifies the action to mirror before being forwarded by the Switch. • *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets

the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

- *rx_rate <value 64-1024000>* – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.

deny – Specifies that packets that do not match the access profile are not permitted to be forwarded by the Switch and will be filtered.

ip – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following:

- *source_ip <ipaddr>* – Specifies that the access profile applies only to packets with this source IP address.
- *protocol_id <value 0-255>* – Specifies that the Switch examine the Protocol field in each packet and if this field contains the value entered here, apply the appropriate rules.
- *destination_ip <ipaddr>* – Specifies that the access profile applies only to packets with this destination IP address.
- *dscp <value 0-63>* – Specifies that the access profile applies only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header.
- *icmp* – Specifies that the Switch examine the protocol field in each frame's header and it should match Internet Control Message Protocol (ICMP).
- *type* – Specifies that the Switch examine each frame's ICMP Type field.
- *code* – Specifies that the Switch examine each frame's ICMP Code field.
- *igmp* – Specifies that the Switch examine each frame's protocol and it should match Internet Group Management Protocol (IGMP) field.
- *type* – Specifies that the Switch examine each frame's IGMP Type field.
- *tcp* - Specifies that the Switch examine each frame's protocol and it should matchTransport Control Protocol (TCP) field.
- *src_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this TCP source port in their TCP header.
- *dst_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this TCP destination port in their TCP header.
- *flag {+ | –} {urg | ack | psh | rst | syn | fin }}* – Specifies the appropriate flag parameter. All incoming packets have TCP flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets.

  To specify flag bits that should be "1" type + and the flag bit name, to specify bits that should be "0" type – and the flag

bit name.

- *udp* – Specifies that the Switch examine the protocol field in each packet and it should match User Datagram Protocol (UDP).
- *src_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this UDP source port in their header.
- *dst_port <value 0-65535>* – Specifies that the access profile applies only to packets that have this UDP destination port in their header.

Ipv6 – Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following:

class <value 0-255> – Examine the class field of IPv6 header. The range is 0 to 255.

source_ipv6 <ipv6addr> – Specifies that the access profile applies only to packets with this source IPv6 address.

destination_ipv6 <ipv6addr> – Specifies that the access profile applies only to packets with this destination IPv6 address.

tcp – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place.

- *src_port <value 0-65535>* – Specifies the TCP source port range. The range is between 0 and 65535.
- *dst_port <value 0-65535>* – Specifies the TCP destination port range. The range is between 0 and 65535.

udp – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place.

- *src_port <value 0-65535>* –Specifies the UDP source port range. The range is between 0 and 65535.
- *dst_port <value 0-65535>* –Specifies the UDP destination port range. The range is between 0 and 65535.

icmp – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place.

- *type <value 0-255>* – Specifies that the Switch examines each frame's ICMP Type field. The range is between 0 and 255.
- *code <value 0-255>* – Specifies that the Switch examines each frame's ICMP Code field. The range is between 0 and 255.

port [<portlist> | *all*| - The access profile for IP may be defined for each port on the Switch.

permit – Specifies that packets that match the access profile are permitted to be forwarded by the Switch.

- *mirror* – Specifies the action to mirror before being forwarded by the Switch.
- *replace_dscp_with <value 0-63>* – Specifies a value to be written to the DSCP field of an incoming packet that meets the criteria specified in the first part of the command. This value will over-write the value in the DSCP field of the packet.

	rx_rate <value 64-1024000> – Specifies the rate limit to limit Rx bandwidth for for the profile being configured. This rate is implemented using the following equation – 1 value = 64kbit/sec. (ex. If the user selects a rx rate limit of 10 then the ingress rate is 640kbit/sec.) The user many select a value between 64- 1024000 or no limit. The default setting is no limit.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the Ethernet access profile:

```
DGS-1210-28MP:5# config access_profile profile_id 2 add access_id 2 ip protocol_id 2 ports 2 deny
Command: config access_profile profile_id 2 add access_id 2 ip protocol_id
 2 ports 2 deny

Success.

DGS-1210-28MP:5#
```

delete access_profile

Purpose	To delete a previously created access profile
Syntax	**delete access_profile [all | profile_id <value 1-50>]**
Description	The **delete access_profile** command deletes a previously created access profile on the Switch.
Parameters	*all* – Specifies all acc profiles to be deleted. *profile_id <value 1-50>* – Specifies the access profile to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the access profile with a profile ID of 1:

```
DGS-1210-28MP:5# delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-1210-28MP:5#
```

show access_profile

Purpose	To display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1-50>}**
Description	The **show access_profile** command displays the currently configured access profiles.
Parameters	*profile_id <value 1-50>* – Specifies the access profile to be displayed. This value is assigned to the access profile when it is created with the **create access_profile** command. If the *profile_id* parameter is omitted, all access profile entries are displayed.

Restrictions	None.

Example usage:

To display the currently configured access profiles which profile id is 1 on the Switch:

```
DGS-1210-28MP:5# show access_profile profile_id 1
Command: show access_profile profile_id 1


Access Profile Table

Access Profile ID: 1          Type: Ethernet
------------------------------------------------------------------------
------------------------------------------------------------------------
Mask Option:
VLAN   802.1p
------------------------------------------------------------------------


DGS-1210-28MP:5#
```

create cpu_access_profile

Purpose	To create an access profile on the Switch by examining the Ethernet part of the packet header. Masks entered are combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**create cpu_access_profile [ethernet {vlan | source_mac <macmask> | destination_mac <macmask> | 802.1p | ethernet_type} | ip {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} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex (0x0-0xffff)>} | protocol_id_mask <hex 0x0-0xff>]} | ipv6 {class | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>}] profile_id <value 1-3>**
Description	The **create cpu_access_profile** command is used to create CPU access list rules on the Switch.
Parameters	*ethernet* - Specifies that the Switch examines the layer 2 part of each packet header with emphasis on one or more of the following: • *vlan* – Specifies a VLAN mask. • *source_mac <macmask >* – Specifies the source MAC mask. • *destination_mac <macmask>* – Specifies the destination MAC mask. • *802.1p* – Specifies 802.1p priority tag mask. *ethernet_type* – Specifies the Ethernet type mask. *ip* - Specifies that the Switch examines the IP fields in each packet with special emphasis on one or more of the following: • *type* – Specifies that the Switch examine each frame's ICMP

	Type field. • *code* – Specifies that the Switch examine each frame's ICMP code field. • *type* – Specifies that the Switch examine each frame's IGMP Type field. *tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place. • *src_port_mask <hex 0x0-0xffff>* – Specifies the TCP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies the TCP port mask for the destination port. • flag_mask - Specifies the appropriate flag. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *src_port_mask <0x0-0xffff>* – Specifies the UDP port mask for the source port. • *dst_port_mask <0x0-0xffff>* – Specifies the UDP port mask for the destination port mask. • *protocol_id_mask <0x0-0xffff>* – Specifies the protocol id mask. • *source_ip_mask <netmask>* – Specifies the source IPv4 mask. • *destination_ip_mask <netmask>* – Specifies the destination IPv4 mask. *dscp* – Specifies that the Switch examines the DiffServ Code Point (DSCP) field in each frame's header. *ipv6* - Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: • *class* – Examine the class field of the IPv6 header. • *source_ipv6_mask <ipv6mask>* – Specifies the source IPv6 mask. • *destination_ipv6_mask < ipv6mask >* – Specifies the destination IPv6 mask. *profile_id <value 1-3>* – Specifies the cpu access profile to be displayed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create a CPU IP access profile:

```
DGS-1210-28MP:5# create cpu access_profile ip source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2
Command: create cpu access_profile ip source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type profile_id 2

Success.
DGS-1210-28MP:5#
```

config cpu_access_profile

Purpose	To configures the settings of cpu access profiles.
Syntax	**config cpu_access_profile [profile_id <value 1-3>] [add access_id [auto_assign | <value 1-5>]] [ethernet {vlan <vlanid 1-4094> | source_mac <macaddr> | destination_mac <macaddr> | 802.1p <value 0-7> | ethernet_type <hex 0x0-0xffff>} | ip {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>] | ipv6 {class | source_ipv6 <ipv6addr> | destination_ipv6 <ipv6addr>} [port [<portlist> | all] [permit | deny]] delete access_id <value 1-5>]**
Description	The **config cpu_access_profile** command configures the settings of cpu access profiles.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be configured. *[add | delete]* – Add or delete the profile id. *access_id [<value 1-5> | auto_assign]* – Specifies the access id value or use auto assign. *ethernet* – Specifies that the Switch examine only the layer 2 part of each packet to determine if it is to be filtered or forwarded based on one or more of the following: • *802.1p <value 0-7>* – Specifies the 802.1p value. The range is between 0 and 7. • *destination_mac <macaddrf>* – Specifies the destination MAC address. • *ethernet_type* – Specifies the Ethernet type mask. • *<portlist>* – Specifies the port or ports to be configured. • *source_mac <macaddr>* – Specifies the source MAC address. *vlan <vlanid 1-4094>* – Specifies the VLAN id. *ip* – Specifies that the Switch examine the IP fields in each packet to determine if it will be either forwarded or filtered based on one or more of the following: • *destination_ip <ip_addr>* – Specifies the destination IP address. • *dscp <value 0-63>* – Specifies the DSCP value. *icmp* – Specifies that the Switch examines the Protocol field in each frame's IP header , and that the value must be 1 (Internet Control Message Protocol- ICMP) for the action to take place. • *code <value 0-255>* –Specifies that the Switch examine each frame's ICMP code field. • *type <value 0-255>* –Specifies that the Switch examine each frame's ICMP Type field. *igmp* – Specifies that the Switch examine each frame's protocol field and it must be 2 (Internet Group Management Protocol-IGMP) for the action to take place. • *igmp_type <value 0-255>* – Specifies the IGMP type. *<portlist>* – Specifies the port or ports to be configured. *protocol_id <value 0-255>* – Specifies the protocol id.

	source_ip <ip_addr> –Specifies that the cpu access profile applies only to packets with this source IP address. *Tcp* – Specifies that the Switch examines each frames protocol field and its value must be 6 (Transmission Control Protocol-TCP) for the action to take place • *dst_port <value 0-65535>* –Specifies that the cpu access profile applies only to packets that have this TCP destination port in their header. • *flag <string>* – Specifies the appropriate flag parameter. • *src_port <value 0-65535>* –Specifies that the cpu access profile applies only to packets that have this TCP source port in their header. *udp* – Specifies that the Switch examines each frame's protocol field and it's value must be 17 (User Datagram Protocol-UDP) in order for the action to take place. • *dst_port <value 0-65535>* – Specifies that the CPU access profile applies only to packets that have this UDP destination port in their header. *src_port <value 0-65535>* – Specifies that the CPU access profile applies only to packets that have this UDP source port in their header. *ipv6* - Specifies that the Switch examines the IPv6 fields in each packet with special emphasis on one or more of the following: • *class* – Examine the class field of the IPv6 header. • *source_ipv6 <ipv6addr>* – Specifies the source IPv6 address. • *destination_ipv6 < ipv6addr >* – Specifies the destination IPv6 address.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a rule for the CPU IP access profile:

```
DGS-1210-28MP:5# config cpu access_profile profile_id 2 add access_id auto_assignip destination_ip 10.48.100.2 ports 1-3 permit
Command: config cpu access_profile profile_id 2 add access_id auto_assign
ip destination_ip 10.48.100.2 ports 1-3 permit

Success.

DGS-1210-28MP:5#
```

delete cpu_access_profile

Purpose	To delete a previously created cpu access profile.
Syntax	**delete cpu_access_profile profile_id <value 1-3>**
Description	The **delete cpu_access_profile** command deletes a previously created access profile on the Switch.
Parameters	*profile_id <value 1-3>* – Specifies the cpu access profile to be deleted.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DGS-1210-28MP:5# delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-1210-28MP:5#
```

show cpu_access_profile

Purpose	To view the CPU access profile entry currently set in the Switch.
Syntax	**show cpu_access_profile {profile_id <value 1-3>}**
Description	The **show cpu access_profile** command is used view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1-3>* – Enter an integer between 1 and 3 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the create cpu access_profile command.
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DGS-1210-28MP:5# show cpu_access_profile
Command: show cpu_access_profile


Access Profile Table

Access Profile ID: 1          Type: Ethernet
--------------------------------------------------------------------------------
--------------------------------------------------------------------------------
Mask Option:
VLAN
--------------------------------------------------------------------------------
DGS-1210-28MP:5#
```

enable cpu_interface_filtering

Purpose	To enable CPU interface filtering on the Switch.
Syntax	**enable cpu_interface_filtering**
Description	The **enable cpu_interface_filtering** command is used to enable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To enable the CPU filtering on the Switch:

```
DGS-1210-28MP:5# enable cpu_interface_filtering
Command: enable cpu_interface_filtering


Success.
DGS-1210-28MP:5#
```

disable cpu_interface_filtering

Purpose	To disable CPU interface filtering on the Switch.
Syntax	**disable cpu_interface_filtering**
Description	The **disable cpu_interface_filtering** command is used to disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To disable the CPU filtering on the Switch:

```
DGS-1210-28MP:5# disable cpu_interface_filtering
Command: disable cpu_interface_filtering


Success.
DGS-1210-28MP:5#
```

40

LINK AGGREGATION COMMANDS

The Link Aggregation commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
create link_aggregation	group_id <value 1-8> {type [lacp | static]}
delete link_aggregation	group_id <value 1-8>
config link_aggregation group_id	<value 1-8> master_port <port 1-28> ports <portlist>
config link_aggregation algorithm	[ip_source | ip_destination | ip_source_dest | mac_source | mac_destination | mac_source_dest]
config link_aggregation state	[enable | disable]
show link_aggregation	{group_id <value 1-8> | algorithm}

Each command is listed in detail, as follows:

create link_aggregation

Purpose	To create a link aggregation group on the Switch.
Syntax	**create link_aggregation group_id <value 1-8> {type [lacp | static]}**
Description	The **create link_aggregation** command creates a link aggregation group with a unique identifier.
Parameters	*group_id* <*value 1-8*> − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This DGSignates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. The maximum ports that can be configure in the same LACP are 16. • *static* – This DGSignates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings. The maximum ports that can be configure in the same static LAG are 8

Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DGS-1210-28MP:5# create link_aggregation group_id 1
Command: create link_aggregation group_id 1

Success.

DGS-1210-28MP:5#
```

delete link_aggregation

Purpose	To delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-8>**
Description	The **delete link_aggregation group_id** command deletes a previously configured link aggregation group.
Parameters	*group_id <value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DGS-1210-28MP:5# delete link_aggregation group_id 1
Command: delete link_aggregation group_id 1


LA channel 1 delete successful
DGS-1210-28MP:5#
```

config link_aggregation group_id

Purpose	To configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-8> master_port <port 1-28> ports <portlist>**
Description	The **config link_aggregation group_id** command configures a link aggregation group created with the **create link_aggregation** command above.
Parameters	*<value 1-8>* − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *master_port <port 1-28>* − Specifies a list of ports to belong to the link aggregation group. Ports will be listed in only one aggregation group and link aggregation groups can not overlap to each other. The user must cofigure at list two ports in LAG. *ports <portlist>* − Specifies a list of ports to belong to the link aggregation group.
Restrictions	Only administrator or operator-level users can issue this command.

Link aggregation groups may not overlap.

Example usage:

To define a load-sharing group of ports, group-id 2 with group members ports 1-5:

```
DGS-1210-28MP:5# config link_aggregation group_id 2 master_port 1 ports 1-5
Command: config link_aggregation group_id 2 master_port 1 ports 1-5

Success.
DGS-1210-28MP:5#
```

config link_aggregation algorithm

Purpose	To configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [ip_source | ip_destination | ip_source_dest | mac_source | mac_destination | mac_source_dest]**
Description	The **config link_aggregation algorithm** 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 using the address-based load-sharing algorithm.
Parameters	*ip_source* − Indicates that the Switch should examine the IP source address. *ip_destination* − Indicates that the Switch should examine the IP destination address. *ip_source_dest* − Indicates that the Switch should examine the IP source and destination addresses. *mac_source* − Indicates that the Switch should examine the MAC source address. *mac_destination* − Indicates that the Switch should examine the MAC destination address. *mac_source_dest* − Indicates that the Switch should examine the MAC source and destination addresses.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure link aggregation algorithm for ip_source:

```
DGS-1210-28MP:5# config link_aggregation algorithm ip_source
Command: config link_aggregation algorithm ip_source

Success.
DGS-1210-28MP:5#
```

config link_aggregation state

Purpose	To enable or disable the link aggregation state.
Syntax	**config link_aggregation state [enable | disable]**
Description	The **config link_aggregation state** command is used to enable or disable the link algorithm feature.

Parameters	*[enable* | *disable]* – Enables or disables the link aggregation state.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable the link aggregation feature:

```
DGS-1210-28MP:5# config link_aggregation state enable
Command: config link_aggregation state enable


LA  Module has been enable
DGS-1210-28MP:5#
```

show link_aggregation

Purpose	To display the current link aggregation configuration on the Switch.
Syntax	**show link_aggregation {group_id <value 1-8> | algorithm}**
Description	The **show link_aggregation** command displays the current link aggregation configuration of the Switch.
Parameters	*group_id* <*value 1-8*> − Specifies the group ID. The Switch allows up to 8 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – shows which hash Algorithm is used for link aggregation distribution.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DGS-1210-28MP:5# show link_aggregation algorithm
Command: show link_aggregation algorithm

Link Aggregation Algorithm = MAC_source


DGS-1210-28MP:5#
```

41

DOS PREVENTION COMMANDS

The DoS Prevention commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config dos_prevention dos_type	[{land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} | all] {action drop} | state [enable | disable]] }
show dos_prevention	{ land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }
enable dos_prevention trap_log	
disable dos_prevention trap_log	

Each command is listed in detail, as follows:

config dos_prevention dos_type	
Purpose	Used to discard the L3 control packets sent to CPU from specific ports.
Syntax	**config dos_prevention dos_type [{land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024} | all] {action drop} | state [enable | disable]] }**
Description	The **config dos_prevention dos_type** command is used to configure the prevention of DoS attacks, and incluDGS state and action. The packets matching will be used by the hardware. For a specific type of attack, the content of the packet, regardless of the receipt port or destination port, will be matched against a specific pattern.
Parameters	The type of DoS attack. Possible values are as follows: land_attack, blat_attack, smurf_attack, tcp_null_scan, tcp_xmascan tcp_synfin and tcp_syn_srcport_less_1024. By default, prevention for all types of DoS are enabled except for tcp_syn_srcport_less_1024. *action [drop | mirror]* - When enabling DoS prevention, the following actions can be taken. · *drop* – Drop the attack packets. · *mirror* – Mirror the packet to other port for further process. *priority <value (0-7)>* – Change packet priority by the Switch from 0 to 7. If the priority is not specified, the original priority will be used. *rx_rate [no_limit | <value (64-1024000)>]* – controls the rate of the received DoS attack packets. If not specified, the default action is

	drop. *state [enable* | *disable]*- Enable or disable DoS prevention.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure a land attack and blat attack prevention:

```
DGS-1210-28MP:5# config dos_prevention dos_type blat_attack action drop
Command: config dos_prevention dos_type blat_attack action drop


Success.

DGS-1210-28MP:5#
```

show dos_prevention

Purpose	Used to display DoS prevention information.
Syntax	**show dos_prevention { land_attack | blat_attack | smurf_attack | tcp_null_scan | tcp_xmascan | tcp_synfin | tcp_syn_srcport_less_1024 }**
Description	The **show dos_prevention** command is used to display DoS prevention information, including the type of DoS attack, the prevention state, the corresponding action if the prevention is enabled, and the counter information of the DoS packet.
Parameters	The type of DoS attack. Possible values are as follows: land_attack, blat_attack, smurf_attack, tcp_null_scan, tcp_xmascan tcp_synfin and tcp_syn_srcport_less_1024.
Restrictions	None.

Example usage:

To display DoS prevention information:

```
DGS-1210-28MP:5# show dos_prevention
Command: show dos_prevention

Trap/Log   : Disabled
DosType                          State      Action       Frame Counts
-------------------------------- ---------- ------------ --------------------
Land Attack                      Enabled    Drop         -
Blat Attack                      Enabled    Drop         -
Tcp Null Scan                    Disabled   Drop         -
Tcp Xmascan                      Disabled   Drop         -
Tcp Synfin                       Enabled    Drop         -
Tcp Syn Srcport less 1024        Enabled    Drop         -
Ping Death Attack                Disabled   Drop         -
Tcp Tiny Fragment                Disabled   Drop         -
```

To display DoS prevention information for Land Attack:

```
DGS-1210-28MP:5# show dos_prevention land_attack
```

```
Command: show dos_prevention land_attack

DoS Type          : Land Attack
  State           : Enabled
  Action          : Drop
  Frame Counts    : -

DGS-1210-28MP:5#
```

enable dos_prevention trap_log

Purpose	Used to enable a DoS prevention trap/log.
Syntax	**enable dos_prevention trap_log**
Description	The **enable dos_prevention trap_log** command is used to send traps and logs when a DoS attack event occurs. The event will be logged only when the action is specified as drop.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable a DoS prevention trap/log:

```
DGS-1210-28MP:5# enable dos_prevention trap_log
Command: enable dos_prevention trap_log

Success.

DGS-1210-28MP:5#
```

disable dos_prevention trap_log

Purpose	Used to disable a DoS prevention trap/log.
Syntax	**disable dos_prevention trap_log**
Description	The **disable dos_prevention trap_log** command is used to disable a DoS prevention trap/log.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable a DoS prevention trap/log:

```
DGS-1210-28MP:5# disable dos_prevention trap_log
Command: disable dos_prevention trap_log

Success.

DGS-1210-28MP:5#
```

42

IP-MAC-PORT BINDING COMMANDS

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC-port binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC-port binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC-port binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the Switch, the maximum value for the IP-MAC-port binding ARP mode is 500. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

The IP-MAC-Port Binding commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table:

Command	Parameter
create address_binding ip_mac	[ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr> ports [<portlist> | all]
config address_binding ip_mac ports	[<portlist> | all] {state [disable | enable] | ip_inspection [disable | enable] | arp_inspection [loose | strict] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}
config address_binding auto_scan	from_ip <ipaddr> to_ip <ipaddr>
config address_binding auto_scan ipv6address	from_ip <ipv6addr> to_ip <ipv6addr>
delete address_binding	[ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr> | all] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <port 1-28>]]
show address_binding	{[ip_mac [all | {ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr>}] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <portlist>]}
show address_binding auto_scan list	
enable address_binding dhcp_snoop	ports [<portlist> | all]
disable address_binding dhcp_snoop	ports [<portlist> | all]
config address_binding dhcp_snoop	{max_entry ports [<portlist> | all] limit [<int 1-10> | no_limit] {IPv6}} | {flush_on_port_down ports <portlist> | all] [enable | disable]}
show address_binding dhcp_snoop	[binding_entry | flust_status | max_entry | vlan_list] ports <portlist>
enable address_binding dhcp_pd_snoop	
disable	

Command	Parameter
address_binding dhcp_pd_snoop	
show address_binding dhcp_pd_snoop	{binding_entry | ports <portlist>}
config address_binding vlan	{<vidlist>} vlan_mode state [enable | disable]
enable address_binding roaming	
disable address_binding roaming	
show address_binding roaming	
clear address_binding dhcp_snoop binding_entry ports	[<portlist> | all] {all | ipv6}

Each command is listed in detail, as follows:

create address_binding ip_mac	
Purpose	Used to create an IP-MAC-port binding entry.
Syntax	**create address_binding ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr>] mac_address <macaddr> ports [<portlist> | all]**
Description	The **create address_binding ip_mac ipaddress** command is used to create an IP-MAC-port binding entry.
Parameters	*ipaddress <ipaddr>* – The IPv4 address of the device where the IP-MAC-port binding is made. *Ipv6address <ipv6addr>* – The IPv4v6 address of the device where the IP-MAC-port binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC-port binding is made. *[<portlist> | all]* – Specifies the ports to be configured for address binding.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To create address binding on the Switch:

```
DGS-1210-28MP:5# create address_binding ip_mac ipaddress 10.90.90.93 mac_address 00-11-11-22-33-44 ports 6
Command: create address_binding ip_mac ipaddress 10.90.90.93 mac_address 00-11-11-22-33-44 ports 6

Success.
DGS-1210-28MP:5#
```

config address_binding ip_mac ports

Purpose	Used to configure an IP-MAC-port binding state to enable or disable for specified ports.
Syntax	**config address_binding ip_mac ports [<portlist> | all] {state [disable | enable] | ip_inspection [disable | enable] | arp_inspection [loose | strict] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}**
Description	The **config address_binding ip_mac ports** command is used to configure the IP-MAC-port binding state to enable or disable for specified ports.
Parameters	*<portlist>* − Specifies a port or range of ports. *all* – Specifies all ports on the switch. *[enable* | *disable]* – Enables or disables the specified range of ports for state, IP-inspection, allow_zeroip and forward_dhcppkt. *arp_inspection [loose* | *strict]* – Specifies to check the ARP inspection to be loose or stict for the specified ports.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding on the Switch:

```
DGS-1210-28MP:5# config address_binding ip_mac ports 3 state disable arp_inspection loose ip_inspection disable
Command: config address_binding ip_mac ports 3 state disable arp_inspection loose ip_inspection disable

Success.
DGS-1210-28MP:5#
```

config address_binding auto_scan

Purpose	Used to configure an IP-MAC-port binding auto scan for specified IP addresses.
Syntax	**config address_binding auto_scan from_ip <ipaddr> to_ip <ipaddr>**
Description	The **config address_binding auto_scan** command is used to configure the IP-MAC-port binding auto scan for specified IP addresses.
Parameters	*<ipaddr>* − Specifies a range of IP addresses for address binding auto scan on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding auto scan on the Switch:

```
DGS-1210-28MP:5# config address_binding auto_scan from_ip 10.0.0.10 to_ip 10.0.0.12
Command: config address_binding auto_scan from_ip 10.0.0.10 to_ip 10.0.0.12

Success.
DGS-1210-28MP:5#
```

config address_binding auto_scan ipv6address

Purpose	Used to configure an IP-MAC-port binding auto scan for specified IPv6 addresses.
Syntax	**config address_binding auto_scan ipv6address from_ip <ipv6addr> to_ip <ipv6addr>**
Description	The **config address_binding auto_scan** command is used to configure the IP-MAC-port binding auto scan for specified IPv6 addresses.
Parameters	*<ipv6addr>* − Specifies a range of IPv6 addresses for address binding auto scan on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure address binding auto scan on the Switch:

```
DGS-1210-28MP:5# config address_binding auto_scan ipv6address from_ip 3000::1 to_ip 3000::3
Command: config address_binding auto_scan ipv6address from_ip 3000::1 to_ip 3000::3

Success.
DGS-1210-28MP:5#
```

delete address_binding

Purpose	Used to delete IP-MAC-port binding entries.
Syntax	**delete address_binding [ip_mac [ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr> | all] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <port 1-28>]]**
Description	The **delete address_binding** command is used to delete IP-MAC-port binding entries. Two different kinds of information can be deleted. *ip_mac* – Individual address binding entries can be deleted by entering the physical and IP addresses of the device. Toggling to all will delete all the address binding entries. *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be deleted by entering the VLAN name and the physical address of the device. To delete all the blocked address binding entries, toggle all.
Parameters	*ipaddress <ipaddr>* – The IPv4 address of the device where the IP-MAC-port binding is made. *iv6paddress <ipv6addr>* – The IPv6 address of the device where the IP-MAC-port binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC-port binding is made. *vlan_name <string 32>* – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *all* – For IP-MAC-port binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all

	the blocked VLANs and their bound physical sddresses. *<port 1-28>* – Specifies a port to be deleted for address binding.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete all address binding entries on the Switch:

```
DGS-1210-28MP:5# delete address_binding ip_mac all
Command: delete address_binding ip_mac all

Success.
DGS-1210-28MP:5#
```

show address_binding

Purpose	Used to display IP-MAC-port binding entries.
Syntax	**show address_binding {[ip_mac [all | {ipaddress <ipaddr> | ipv6address <ipv6addr> | mac_address <macaddr>}] | blocked [all | vlan_name <string 32> mac_address <macaddr> port <portlist>]}**
Description	This **show address_binding** command is used to display IP-MAC-port binding entries. Four different kinds of information can be viewed. *ip_mac* – Address binding entries can be viewed by entering the physical and IP addresses of the device. *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. *ports* – The number of enabled ports on the device.
Parameters	*ip_mac* – The database the user creates for address binding. *all* – For IP MAC binding all specifies all the IP-MAC-port binding entries; for blocked address binding entries all specifies all the blocked VLANs and their bound physical addresses. *blocked* – The address database that the system auto learns and blocks. *ipaddress <ipaddr>* – The IPv4 address of the device where the IP-MAC-port binding is made. *ipv6address <ipv6addr>* – The IPv6 address of the device where the IP-MAC-port binding is made. <*macaddr*> – The MAC address of the device where the IP-MAC-port binding is made. *vlan_name <string 32>* – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN. *port <portlist>* – Specifies a port to be displayed for the address binding on the Switch.
Restrictions	None.

Example usage:

To display address binding entries on the Switch:

```
DGS-1210-28MP:5# show address_binding ip_mac all
Command: show address_binding ip_mac all
```

```
IP Address      MAC Address        Port
--------------  -----------------  ----
10.0.0.21       00-00-00-00-01-02  3

DGS-1210-28MP:5#
```

show address_binding auto_scan list

Purpose	Used to display IP-MAC-port binding entries.
Syntax	**show address_binding auto_scan list**
Description	This **show address_binding auto_scan list** command is used to display auto scan list of address binding on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the auto scan list of address binding on the Switch:

```
DGS-1210-28MP:5# show address_binding auto_scan list
Command: show address_binding auto_scan list

VLAN IP Address                      MAC Address        Port  Bound
--------- ---------------------------------- ------------------ ------ -----------

Total Entries : 0
DGS-1210-28MP:5#
```

enable address_binding dhcp_snoop

Purpose	Used to enable address binding DHCP Snooping.
Syntax	**enable address_binding dhcp_snoop ports [<portlist> | all]**
Description	This **enable address_binding dhcp_snoop** command is used to enable IP-MAC-port binding DHCP snooping entries.
Parameters	*[<portlist> | all]* – Specifies a port, a range of ports or all ports to be enabled of the address binding DHCP snooping on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the DHCP snooping of address binding for port 3~5 on the Switch:

```
DGS-1210-28MP:5# enable address_binding dhcp_snoop ports 3-5
Command: enable address_binding dhcp_snoop ports 3-5

Success.
DGS-1210-28MP:5#
```

disable address_binding dhcp_snoop

Purpose	Used to disable address binding DHCP Snooping.
Syntax	**disable address_binding dhcp_snoop ports [<portlist> | all]**
Description	This **disable address_binding dhcp_snoop** command is used to disable IP-MAC-port binding DHCP snooping entries.
Parameters	*[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be enabled of the address binding DHCP snooping on the Switch.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the DHCP snooping of address binding for port 3~5 on the Switch:

```
DGS-1210-28MP:5# disable address_binding dhcp_snoop ports 4
Command: disable address_binding dhcp_snoop ports 4

Success.
DGS-1210-28MP:5#
```

config address_binding dhcp_snoop

Purpose	Used to configure the max entry and entry reflush mechanism of DHCP snooping function..
Syntax	**config address_binding dhcp_snoop {max_entry ports [<portlist> | all] limit [<int 1-10> | no_limit] {IPv6}} | {flush_on_port_down ports <portlist> | all] [enable | disable]}**
Description	The **config address_binding dhcp_snoop max_entry** command is used to specify the maximum number of DHCP snooping entries on specified ports. By default, the per-port maximum entry has no limit. The command **config address_binding dhcp_snooping flush_on_port_dow**n command forces to clear binded entry when port physical state is down.
Parameters	*max_entry* – The max binding entry of DHCP snooping *[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be configured of the address binding DHCP snooping on the Switch. *[<int 1-10>* | *no_limit]* – Specifies the limit for max entry number. *{IPv6}* – Specifies the IPv6 address used for this configuration. *Flush_on_port_down* – The mechanism to force clear binded entry when the specified port physically down. *[<portlist>* | *all]* – Specifies a port, a range of ports or all ports to be configured. *enable* | *disable* – Specified the state
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To configure the DHCP snooping of address binding for port 1 on the Switch:

```
DGS-1210-28MP:5# config address_binding dhcp_snoop max_entry ports 1 limit 1
Command: config address_binding dhcp_snoop max_entry ports 1 limit 1

Success.
```

```
DGS-1210-28MP:5#
DGS-1210-28MP:5# config address_binding dhcp_snoop flush_on_port_down ports 1 enable
Command: config address_binding dhcp_snoop flush_on_port_down ports 1 enable

Success.
```

show address_binding dhcp_snoop

Purpose	Used to display DHCP snoop of IP-MAC-port binding.
Syntax	**show address_binding dhcp_snoop [binding_entry | flush_status | max_entry | vlan_list] {ports <portlist>}**
Description	This command is used show types information about DHCP snooping which includes binding entry, flush status, max entry a nd vlan list.
Parameters	*binding_entry* – Display the binding entry *flush_status* – Display the configured status of flush_on_port_down feature *max_entry* - Specifies ddress binding entries can be viewed. *vlan_list* – Display the list of VLAN group that configured to turn on DHCP snooping. *ports <portlist>* – Specifies the ports on the device to be displayed.
Restrictions	None.

Example usage:

To display DHCP snoop of address binding max entries of port 1~5 on the Switch:

```
DGS-1210-28MP:5# show address_binding dhcp_snoop max_entry ports 1-5
Command: show address_binding dhcp_snoop max_entry ports 1-5

Port  Max Entry       Max IPv6 Entry
----  --------------- ----------------------
1     No Limit        No Limit
2     No Limit        No Limit
3     No Limit        No Limit
4     No Limit        No Limit
5     No Limit        No Limit
DGS-1210-28MP:5#
```

enable address_binding dhcp_pd_snoop

Purpose	Used to enable address binding DHCPv6 PD Snooping.
Syntax	**enable address_binding dhcp_pd_snoop**
Description	This **enable address_binding dhcp_pd_snoop** command is used to enable IP-MAC-port binding DHCPv6 PD snooping.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable address binding DHCPv6 PD Snooping on the Switch:

```
DGS-1210-28MP:5# enable address_binding dhcp_pd_snoop
Command: enable address_binding dhcp_pd_snoop

Success.
DGS-1210-28MP:5#
```

disable address_binding dhcp_pd_snoop

Purpose	Used to disable address binding DHCPv6 PD Snooping.
Syntax	**disable address_binding dhcp_pd_snoop**
Description	This **disable address_binding dhcp_pd_snoop** command is used to disable IP-MAC-port binding DHCPv6 PD snooping.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable address binding DHCPv6 PD Snooping on the Switch:

```
DGS-1210-28MP:5# disable address_binding dhcp_pd_snoop
Command: disable address_binding dhcp_pd_snoop

Success.
DGS-1210-28MP:5#
```

show address_binding dhcp_pd_snoop

Purpose	Used to display address binding DHCPv6 PD Snooping.
Syntax	**show address_binding dhcp_pd_snoop {binding_entry | ports <portlist>}**
Description	This **show address_binding dhcp_pd_snoop** command is used to display IP-MAC-port binding DHCPv6 PD snooping.
Parameters	None.
Restrictions	None.

Example usage:

To display address binding DHCPv6 PD Snooping on the Switch:

```
DGS-1210-28MP:5# show address_binding dhcp_pd_snoop binding_entry
Command: show address_binding dhcp_pd_snoop binding_entry

IP Address                      Port Lease  Remain
--------------------------------------- ------- ---------- ------------



Total Entries  : 0

DGS-1210-28MP:5#
```

config address_binding vlan

Purpose	Used to configure an IP-MAC-port binding specified VLAN.
Syntax	**config address_binding vlan {<vidlist>} vlan_mode state [enable | disable]**
Description	The **config address_binding vlan** command is used to configure the IP-MAC-port binding for specified VLAN.
Parameters	*{<vidlist>}* − Specifies the VLAN ID to be configured. [*enable* | *disable]* – Specifies to enable or disable the IP-MAC-port binding of the specified VLAN.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the address binding of VLAN ID 1on the Switch:

```
DGS-1210-28MP:5# config address_binding vlan 1 vlan_mode state disable
Command: config address_binding vlan 1 vlan_mode state disable

Success.
DGS-1210-28MP:5#
```

enable address_binding roaming

Purpose	Used to enable address binding roaming.
Syntax	**enable address_binding roaming**
Description	This **enable address_binding roaming** command is used to enable IP-MAC-port binding roaming.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To enable the roaming of address binding on the Switch:

```
DGS-1210-28:5# enable address_binding roaming
Command: enable address_binding roaming

Success.
DES-1210-52:5#
```

disable address_binding roaming

Purpose	Used to disable address binding roaming.
Syntax	**disable address_binding roaming**
Description	This **disable address_binding roaming** command is used to disable IP-MAC-port binding roaming.
Parameters	None.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To disable the roaming of address binding on the Switch:

```
DGS-1210-28:5# disable address_binding roaming
Command: disable address_binding roaming

Success.
DES-1210-52:5#
```

show address_binding roaming

Purpose	Used to display DHCP snoop of IP-MAC-port binding lroaming information.
Syntax	**show address_binding roaming**
Description	This **show address_binding roaming** command is used to display DHCP snoop of IP-MAC-port binding roaming information.
Parameters	None.
Restrictions	None.

Example usage:

To display DHCP snoop of address binding roaming information on the Switch:

```
DGS-1210-28:5# show address_binding roaming
Command: show address_binding roaming

Roaming state is enabled.
DES-1210-52:5#
```

clear address_binding dhcp_snoop binding_entry ports

Purpose	Used to clear the DHCP snooping entries learned for the specified ports.
Syntax	**clear address_binding dhcp_snoop binding_entry ports [<portlist> | all] {all | ipv6}**
Description	This **clear address_binding dhcp_snoop binding_entry ports** command is used to clear the DHCP snooping entries learned for the specified ports.
Parameters	*[<portlist> | all]* – Specifies a range of ports or all ports to be configured. *all* - Specifies that all entries will be cleared. *ipv6* - Specifies that IPv6 entries will be cleared.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To clear DHCP IPv4 snooping entries on ports 1-3:

```
DGS-1210-28MP:5# clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.
DGS-1210-28MP:5#
```

43

POE COMMANDS

The PoE commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameter
config poe ports	[all | <portlist>] {clear_time_range | power_limit [auto | class_1 | class_2 | class_3 | class_4 | user_define <value 1-30>] | priority [high | normal | low] | state [enable | disable] | time_range <range_name 32>}
config por system	[legacy_pd [enable | disable] | power_disconnect_method [deny_low_priority_port | deny_next_port] | power_limit <sting>]
show poe ports	[all | <portlist>]
show poe system	

Each command is listed in detail, as follows:

config poe ports

Purpose	Used to configure the Power over Ethernet (PoE) functionality.
Syntax	**config poe ports [all | <portlist>] [state {enable | disable}] [time_range <range_name 32> | clear_time_range | priority {High | Normal | low} | power_limit {Auto | class_1 | class_2 | class_3 | class_4 | user_define <value 1-30>} | delay_power_detect {enable | disable}]**
Description	The config poe ports configures the Power over Ethernet (PoE) functionality of the Switch.
Parameters	*port* – Specify the port(s) for PoE parameters *all* – Specify all ports <*portlist*> − Specify the port, or a range of ports. *state* –Specifies whether power will be supplied to the powered device connected to this port or not *enable* - Specifies that PoE will be enabled of the specifies port(s). *disable* - Specifies that PoE will be disabled of the specifies port(s). *time_range <range_name 32>* - To configure the time-based PoE function on designated port(s). *clear_time_range* – Used to delete the time range for specified port(s). *priority* - Port priority determines the priority the system attempts to supply the power to the port. *High* –Specifies that the priority value will be set to high. *Normal* –Specifies that the priority value will be set to normal. *Low* - Specifies that the priority value will be set to low. *power_limit* - Specifies the power limit with different class *auto* –Automatic classification the PD's power consumption.

	class_1 - Specifies that the power limit will be set to 4W *class_2* - Specifies that the power limit will be set to 7W *class_3* - Specifies that the power limit will be set to 15.4W *class_4* –For 802.3at compliance PD devices. Supports up to 30W in this class. *user_define <value 1-30>* –Specifies the user defined power limit value here. Maximum capability for power output is 30W (802.3AT)
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure PoE with ports 8-10:

DGS-1210-28MP:5# config poe ports 8-10 power_limit Auto priority low state enable

Command: config poe ports 8-10 power_limit Auto priority low state enable

Success!

DGS-1210-28MP:5#

config poe system

Purpose	Used to configure the Power over Ethernet (PoE) parameter for entire system.
Syntax	**config poe system [legacy_pd [enable | disable] | power_disconnect_method [deny_low_priority_port | deny_next_port] | power_limit <string>]**
Description	The config poe system configures the Power over Ethernet (PoE) functionality of the Switch.
Parameters	*legacy_pd* - Specifies the legacy PDs detection status. *enable* - Specifies that the legacy PDs detection status will be enabled. *disable* − Specifies that the legacy PDs detection status will be disabled and can't detect the legacy PDs signal. *power_disconnect_method* - Specifies the disconnection method that will be used when the power budget is running out. *deny_low_priority_port* - The port with the lower priority will be shut down to allow the higher priority port to power up. *deny_next_port* - When the power budget is exceeded, the next port attempting to power up is denied, regardless of the port priority. *power_limit <string>* - Configure the system power budge.Different mdoel has different power limit. Please refer to hardware specification.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure PoE with ports 8-10:

```
DGS-1210-28MP:5# config poe system power_limit 193
Command: config poe system power_limit 193



Success!

DGS-1210-28MP:5#
```

show poe ports

Purpose	Used to display the ports of Power over Ethernet (PoE).
Syntax	**show poe ports [all | <portlist>]**
Description	The show poe ports displays the Power over Ethernet (PoE) ports of the Switch.
Parameters	*[all* | *<portlist>]* – Specifies the ports or all ports to be displayed.
Restrictions	None.

Example usage:

To display the PoE with ports 8:

```
DGS-1210-28MP:5# show poe ports 8
Command: show poe ports 8



Port: 8
State                : Enable
Priority             : Low
Power Limit          : Auto
Power(W)             : 0.0
Voltage(V)           : 0.0
Current(mA)          : 0.0
Status               : POWER OFF
Time Range           : N/A

Success!

DGS-1210-28MP:5#
```

show poe system

Purpose	Used to display the system information of Power over Ethernet (PoE).
Syntax	**show poe system**
Description	The show poe system displays the Power over Ethernet (PoE) system information of the Switch.
Parameters	None.

Restrictions	None.

Example usage:

To display the PoE system of Switch:

```
DGS-1210-28MP:5# show poe system
Command: show poe system

Power Limit                    : 193
Power Consumption              : 0
Power Remained                 : 0
Power Disconnection Method     : Deny Next Port
Detection Legacy PD            : Disable

Success!

DGS-1210-28MP:5#
```