D-Link
Building Networks for People

CLI Reference Guide

Product Model : **DGS-1100-06/ME**
Metro Ethernet Managed Switch
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。

Oct, 2012

Table of Contents

1

INTRODUCTION

The DGS-1100-06/ME consists of 5 10/100/1000Mbps ports plus 1 100/100/SFP port.

The Switch can be managed through the Telnet or the Web-based management agent. The Command Line Interface (CLI) can be used to configure and manage the Switch via the 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 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-1100-06/ME:5# config ipif System ipaddress 10.90.90.91/8
Command: config ipif System ipaddress 10.90.90.91/8

% The IP setting mode change to static will cause CLI disconnect.
DGS-1100-06/ME:5# _
```

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.

After the Switch reboots and you have to logged in, the console looks like this:

```
DGS-1100-06/ME Gigabit Ethernet Switch
Command Line Interface

Copyright(C) 2012 D-Link Corporation. All rights reserved.

DGS-1100-06/ME login:
```

Figure 2–1 Initial Console Screen after Logging In

Commands are entered at the command prompt, DGS-1100-06/ME: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.

```
Command: ?


?
cable diagnostic port
clear arptable
clear counters
clear ethernet_oam ports
clear flood_fdb
clear igmp_snooping statistics counter
clear log
clear mld_snooping statistics counter
config 802.1x auth_mode ports
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x fwd_pdu system
config 802.1x guest_vlan ports
config 802.1x init port_based ports
config 802.1x reauth port_based ports
config account
config admin local_enable
config arp_aging time
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL_
```

Figure 2–2 The ? Command

When entering a command without its required parameters, the CLI displays the prompt: command: config account message and the options listed below.

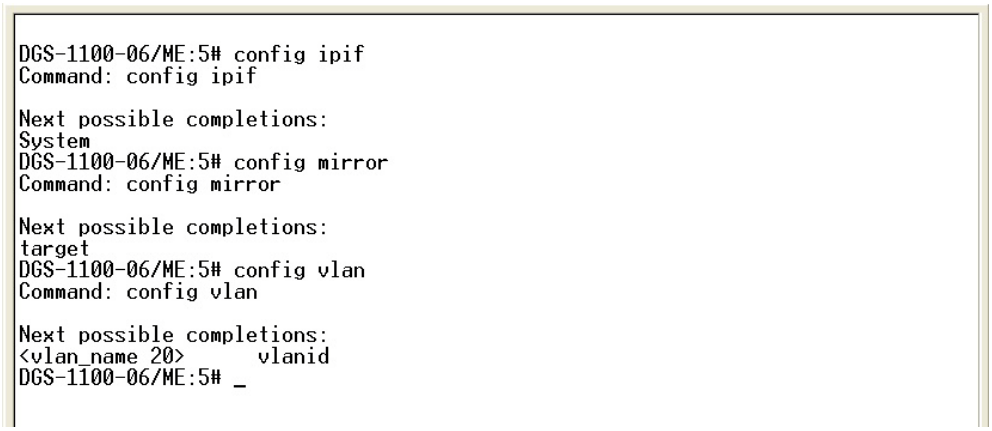

Figure 2–3 Example Command Parameter Help

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.

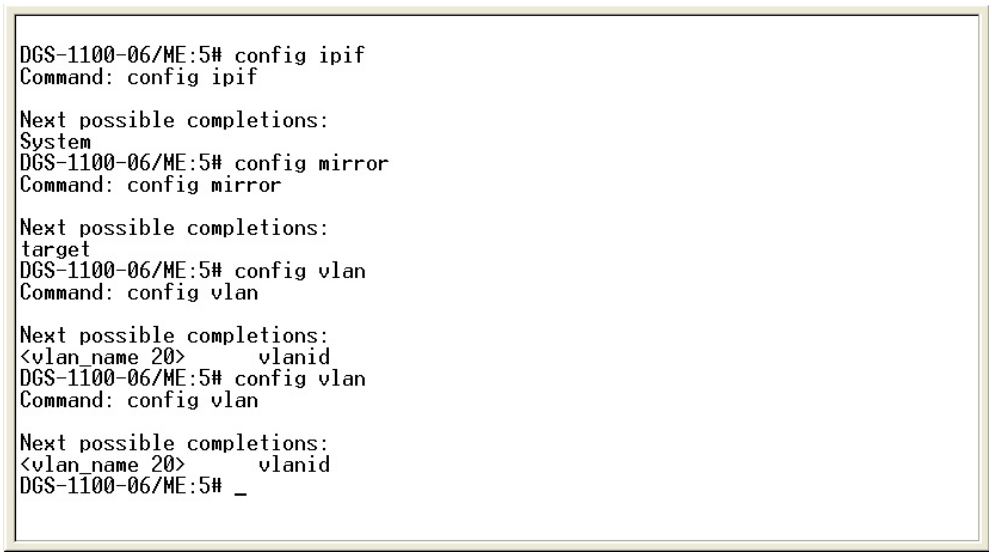

Figure 2–4 Using the Up Arrow to Re-enter a Command

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: prompt.

```
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5#
DGS-1100-06/ME:5# ask
Available commands:
?                   cable               clear               config

create              delete              disable             download

enable              logout              ping                ping6

reboot              reload              reset               save

show                upload
DGS-1100-06/ME: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.

```
igmp_snooping       ipif                lacp
limited_multicast_addr                  link_aggregation    lldp

log                 log_save_timing     loopdetect          mac_notification

management          max_mcast_group     mcast_filter_profile

mirror              multicast           multicast_fdb       packet

port_security       ports               pppoe               qinq

radius              rmon                router_ports        safeguard_engine

scheduling          scheduling_mechanism                    session

smart_binding       smtp                snmp                sntp

ssh                 ssl                 stp                 switch

syslog              tech                time                traffic

traffic_segmentation                    trusted_host        uplink

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

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>
show account	
delete account	<username 15>
save account	
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 auto learning	
disable auto learning	
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	
save	{[config config_id <value 1-2> | log | account]}
reboot	
reset	{[config | system | account | password]} {force_agree}
logout	
ping	<ipaddr> {times <value 1-255> | timeout <sec 1-99> | size <short 0-2080>}
ping6	<ipv6_addr> {frequency <sec 0-86400> | size <value 1-1522> | source_ip <ipv6_addr> | timeout <sec 1-99> | times <value 1-255>}
enable telnet	

Command	Parameter
disable telnet	
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	
show tech support	

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-1100-06/ME:5# enable password encryption
Command: enable password encryption


Success.

DGS-1100-06/ME: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-1100-06/ME:5# disable password encryption
Command: disable password encryption


Success.

DGS-1100-06/ME:5#
```

create account

Purpose	To create user accounts.
Syntax	create account [admin | operator | user | poweruser] <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. *poweruser* − Specify a power user level account. *<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-1100-06/ME: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-1100-06/ME:5#
```

config account

Purpose	To change the password for an existing user account.
Syntax	config account <username 15>
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.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user password of 'dlink' account:

```
DGS-1100-06/ME:5# config account dlink
Command: config account dlink


Enter a old password:***

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

Success.

DGS-1100-06/ME:5#
```

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 account which have been created:

```
DGS-1100-06/ME:5# show account
Command: show account


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

Total Entries : 1

DGS-1100-06/ME: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-1100-06/ME:5# delete account System
Command: delete account System

Success.

DGS-1100-06/ME:5#
```

save account

Purpose	To save an existing user account.
Syntax	save account
Description	The save account command saves all user account that has been created using the create account command.
Parameters	None..
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To save the all user accounts:

```
DGS-1100-06/ME:5# save account
Command: save account

DGS-1100-06/ME:5#
```

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 the way users logged in:

```
DGS-1100-06/ME:5# show session
Command: show session

Total Entries: 1

ID  Login Time            Live Time   From          Level    Name
--  ----------------------  ----------   ---------------   -----    ---------------
0   Jan  1 01:04:08 2012   00:11:05                    14       root

Total Entries: 1



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

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-1100-06/ME:5# show switch
Command: show switch

System name                :
System Contact             :
System Location            :
```

```
System up time                  : 0 days, 0 hrs, 20 min, 28 secs
System Time                     : 01/01/2012 00:20:30
System hardware version         : A1
System firmware version         : 1.00.008
System boot version             : 1.00.000
System Protocol version         : 2.001.004
System serial number            : 1MB1733K0000A
MAC Address                     : 00-AE-B7-21-22-62
SNMP Status                     : Enabled
Port Mirroring                  : Disabled
802.1X Status                   : Disabled
Storm Control                   : Disabled
802.1Q Management VLAN          : Disabled
Safeguard Engine                : Enabled
IGMP Snooping                   : Disabled

DGS-1100-06/ME: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 and configure the TCP port number to listen for Telnet requests:

```
DGS-1100-06/ME:5# enable web
Command: enable web

Success.

DGS-1100-06/ME: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.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable HTTP-based management software on the Switch:

```
DGS-1100-06/ME:5# disable web
Command: disable web

Success.

DGS-1100-06/ME: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, the Switch becomes a DHCP client automatically (same as: config ipif System dhcp). The DHCP server must have the TFTP server IP address and configuration file name, and be configured to deliver this information in the data field of the DHCP reply packet. The TFTP server must be running and have the requested configuration file in its base directory when the request is received from the Switch. Consult the DHCP server and TFTP server software instructions for information on loading a configuration file. If the Switch is unable to complete the auto configuration process the previously saved local configuration file present in Switch memory will be loaded.

Example usage:

To enable auto configuration on the Switch:

```
DGS-1100-06/ME:5# enable autoconfig
Command: enable autoconfig



Success.
DGS-1100-06/ME: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-1100-06/ME:5# disable autoconfig
Command: disable autoconfig


Success.
DGS-1100-06/ME: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-1100-06/ME:5# show autoconfig
Command: show autoconfig

Autoconfig State: Enabled

DGS-1100-06/ME: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] <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] − Display the configuration which is begined or excluded. <string 80> − Display the configuration which begin or exclude the specified string. The maximum string is 80.
Restrictions	None.

Example usage:

To display the autoconfig status:

```
#------------------------------------------------------------------------------------------------
#            DGS-1100-06/ME Gigabit Ethernet Switch Configuration
#
#                        Firmware: Build 1.00.011
#       Copyright(C) 2010 D-Link Corporation. All rights reserved.
#------------------------------------------------------------------------------------------------
command-start

# Basic
config syslogintimeout 5
config sysgroupinterval 120
enable web 80
config arp_aging time 5
config fdb aging_time 300
enable telnet 23

# Vlan
disable asymmetric_vlan
create vlan default
config vlan vlanid 1 add untagged 1-6
config multicast filter 1 forward
config multicast filter 2 forward
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a ALL
```

enable auto learning

Purpose	To enable the MAC address auto learning on the switch.
Syntax	enable auto learning
Description	The **enable auto learing** command enables the MAC address auto learning feature on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable auto learning on the Switch:

```
DGS-1100-06/ME:5# enable auto learning
Command: enable auto learning



Success
DGS-1100-06/ME:5#
```

disable auto learning

Purpose	To disable the MAC address auto learning of the switch.
Syntax	**disable auto learning**

Description	The **disable auto learing** command disables the MAC address auto learning feature on the Switch.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable auto learning on the Switch:

```
DGS-1100-06/ME:5# disable auto learning
Command: disable auto learning



Success
DGS-1100-06/ME:5#
```

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. Jumbo frames will be enabled after save and restart.

Example usage:

To enable jumbo frames:

```
DGS-1100-06/ME:5# enable jumbo_frame
Command: enable jumbo_frame.



Success.
DGS-1100-06/ME: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. Jumbo frames will be disabled after save and restart.

Example usage:

To disable jumbo_frames:

```
DGS-1100-06/ME:5# disable jumbo_frame
```

```
Command: disable jumbo_frame



Success.

DGS-1100-06/ME: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 configuration status on the device:

```
DGS-1100-06/ME:5# show jumbo_frame
Command: show jumbo_frame



Jumbo frame is enable.

Success
DGS-1100-06/ME:5#
```

save	
Purpose	To save changes in the Switch's configuration to non-volatile RAM.
Syntax	save {[config config_id <value 1-2> | log | account]}
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. *config_id <value 1-2>* - Specifies which cfg file ID if cfg ID is not specified, it refers to the boot_up CFG file. *log* – Used to save the current log to a file. The log file cannot be deleted. *account* – Used to save the account to a file.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To save the Switch's current configuration to non-volatile RAM:

```
DGS-1100-06/ME:5# save
Command: save

Building configuration ...
[OK]
DGS-1100-06/ME: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-1100-06/ME:5# reboot
Command: reboot


Are you sure you want to proceed with the system reboot? (y/n)y
% Please wait, the switch is rebooting...
DGS-1100-06/ME:5#
DGS-1100-06/ME:5# System will Reboot....


 Boot Procedure
--------------------------------------------------------------------------------


PP_init for CAMEO DGS-1100-06ME(instead of EEPROM)
 Please wait, loading Runtime image ..........  100%

 MAC Address : 00-AE-B7-21-22-62
 H/W Version : Rev.A1
 F/W Version : 1.00.008

 ........................................

            DGS-1100-06/ME Gigabit Ethernet Switch
                 Command Line Interface

        Copyright(C) 2012 D-Link Corporation. All rights reserved.

DGS-1100-06/ME login:
```

reset	
Purpose	To reset the Switch to the factory default settings.
Syntax	reset {[config | system | account | password]} {force_agree}
Description	The reset command restores the Switch's configuration to the default settings assigned from the factory.
Parameters	*config* - If the keyword 'config' is specified, all of the factory default settings are restored on the Switch including the IP address, user accounts, and the switch history log. The Switch will not save or reboot. *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. Rebooting will clear all entries in the Forwarding Data Base. *account* − If the keyword 'account is specified, all of the factory default account settings are restored on the Switch. *password* − If the keyword 'password is specified, all of the factory default password settings are restored on the Switch. *{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-1100-06/ME:5# reset system
Command: reset system


Are you sure you want to proceed with the system reset, save and reboot?(y/n)y
% Success.
DGS-1100-06/ME:5# System will Reboot....


  Boot Procedure
--------------------------------------------------------------------------------
PP_init for CAMEO DGS-1100-06ME(instead of EEPROM)
  Please wait, loading Runtime image ..........  100%

  MAC Address : 00-AE-B7-21-22-62
  H/W Version : Rev.A1
  F/W Version : 1.00.008

  ..............................................

            DGS-1100-06/ME Gigabit Ethernet Switch
                 Command Line Interface

        Copyright(C) 2012 D-Link Corporation. All rights reserved.

DGS-1100-06/ME login:
```

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 user's Telnet session:

```
DGS-1100-06/ME:5# logout
```

ping

Purpose	To test the connectivity between network devices.
Syntax	ping <ipaddr> {times <value 1-255> | timeout <sec 1-99> | size <short 0-2080>}
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 1-255>* - 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 <short 0-2080>* - 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 10.6.150.34 three times:

```
DGS-1100-06/ME:5#ping 10.6.150.34 times 3
Command: ping 10.6.150.34 times 3

Reply Not Received From : 10.6.150.34, Timeout : 5 secs
Reply Not Received From : 10.6.150.34, Timeout : 5 secs
Reply Not Received From : 10.6.150.34, Timeout : 5 secs

--- 10.6.150.34 Ping Statistics ---
3 Packets Transmitted, 0 Packets Received, 100% Packets Loss
DGS-1100-06/ME:5#
```

ping6

Purpose	To test the IPv6 connectivity between network devices.
Syntax	ping6 <ipv6_addr> {frequency <sec 0-86400> | size <value 1-1522> | source_ip <ipv6_addr> | 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	*<ipv6_addr>* - The IPv6 address of the host. *frequency <sec 0-86400>* - The number of seconds to wait before repeating a ping test as defined by the value of this parameter. A single ping test consists of a series of ping probes. The number of probes is determined by the value of the parameter times. After a single test completes the number of seconds as defined by the value of frequency must elapse before the next ping test is started. A value of 0 for this parameter implies that the test as defined by the corresponding entry will not be repeated. *size <value 1-1522>* - Specify the size of the test packet. A value of 1 to 1522 can be specified. *source_ip <ipv6_addr >* - Specify the source IPv6 address of the ping packets. If specified this parameter, this IPv6 address will be used as the packets' source IPv6 address that ping6 sends to the remote host.

	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-1100-06/ME: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-1100-06/ME:5#
```

enable telnet

Purpose	To enable the telnet.
Syntax	enable telnet
Description	The **enable** telnet command enables telnet.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command

Example usage:

To enable telnet:

```
DGS-1100-06/ME:5#enable telnet
Command: enable telnet


Success.
DGS-1100-06/ME:5#
```

disable telnet

Purpose	To disable telnet.
Syntax	disable telnet
Description	The **disable telnet** command disables telnet.
Parameters	None.
Restrictions	Only Administrator or operate-level users can issue this command

Example usage:

To disable telnet:

```
DGS-1100-06/ME:5#disable telnet
Command: disable telnet

Success.

DGS-1100-06/ME:5#
```

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 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]
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 2011-2029 >* – 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 2011-2029 >* – 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-1100-06/ME:5# config time_range dd hours start_time 00:22 end_time
12:34 weekdays tue-fri date from_day year 2012 month 1 date 1 to_day year
2012 month 1 date 3
Command: config time_range dd hours start_time 00:22 end_time 12:34
weekdays tue-fri date from_day year 2012 month 1 date 1 to_day year 2012
month 1 date 3



Success!

DGS-1100-06/ME:5#
```

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-1100-06/ME:5# show time_range

Range name    : xxx
Start time    : 10:00
End time      : 11:00
Days          : wed sun

Total Entries : 1

DGS-1100-06/ME:5#
```

show tech support

Purpose	To display system and configuration information. to provide to the Technical Assistance Center when reporting a problem, use the show tech-support command.
Syntax	show tech support
Description	The show tech support command displays system and configuration information. to provide to the Technical Assistance Center when reporting a problem. By default, this command displays the output for technical-support-related show commands. Use keywords to specify the type of information to be displayed. If you do not specify any parameters, the system displays all configuration and memory data. The **show tech support** command may time out if the configuration file output takes longer to display than the configured session timeout time. If this happens, enter a set logout *timeout* value of 0 to disable automatic disconnection of idle sessions or enter a longer *timeout* value. The **show tech support** command output is continuous; it does not display one screen at a time. To interrupt the output, press Esc.
Parameters	None.
Restrictions	None.

Example usage:

To display technical support information on the Switch:

```
DGS-1100-06/ME:5#show tech support

Command: show tech support

- System Info. -
```

```
System name                    :
System Contact                 :
System Location                :
System up time                 : 0 days, 0 hrs, 7 min, 12 secs
System Time                    : 01/01/2012 00:07:14
System hardware version        : A1
System firmware version        : 1.00.008
System boot version            : 1.00.000
System Protocol version        : 2.001.004
System serial number           : 1MB1733K0000A
MAC Address                    : 00-AE-B7-21-22-62
SNMP Status                    : Enabled
Port Mirroring                 : Disabled
802.1X Status                  : Disabled
Storm Control                  : Disabled
802.1Q Management VLAN         : Disabled
Safeguard Engine               : Enabled
IGMP Snooping                  : Disabled

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

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-1100-06/ME". *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:

To modify the command prompt to "AtYourService":

```
DGS-1100-06/ME:5#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService: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. Only valid in threshold level.

Example usage:

```
To the banner:DGS-1100-06/ME:5#
Command: config greeting_message

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

                DGS-1100-06/ME Gigabit Ethernet Switch
                   Command Line Interface

          Copyright(C) 2012 D-Link Corporation. All rights reserved.
=============================================================


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

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-1100-06/ME:5#show greeting_message
Command: show greeting_message


                DGS-1100-06/ME Gigabit Ethernet Switch
                   Command Line Interface

          Copyright(C) 2012 D-Link Corporation. All rights reserved.

DGS-1100-06/ME: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_100 | fiber_1G] MDI/MDIX [MDI | MDIX | auto] {description <desc 32> | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 10_half | 100_full | 100_half | 10_full | 10_half]}
delete ports	[<portlist> | all] medium_type [copper | fiber_100 | fiber_1G] description
show ports	{<portlist> | all} {description | err_disabled}
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_100 | fiber_1G] MDI/MDIX [MDI | MDIX | auto] {description <desc 32> | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | speed [auto | 1000_full | 10_half | 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_100 | fiber_1G]* − 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. *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 operate-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-1100-06/ME: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-1100-06/ME:5#
```

delete ports

Purpose	To delete the description of current configuration port.
Syntax	delete ports [<portlist> | all] medium_type [copper | fiber_100 | fiber_1G] description
Description	The delete ports command deletes the description of current configuration port or range of ports.
Parameters	*[<portlist> | all]* − All port or range of ports whose settings are to be removed. *medium_type [copper | fiber_100 | fiber_1G]* − If configuring the Combo ports, this description the type of medium being removed.
Restrictions	Only administrator or operate-level users can issue this command.

Example usage:

To delete the description of port 3 on the Switch:

```
DGS-1100-06/ME:5# delete ports 3 medium_type copper description
Command: delete ports 3 medium_type copper description

DGS-1100-06/ME:5#
```

show ports

Purpose	To display the current configuration of a range of ports.
Syntax	show ports {<portlist> | all} {description | err_disabled}
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.

Restrictions	None.

Example usage:

To display the configuration of port 3 on the Switch:

```
DGS-1100-06/ME:5# show ports 3
Command: show ports 3


Port  State/     Settings                 Connection               Address
Type  MDI        Speed/Duplex/FlowCtrl    Speed/Duplex/FlowCtrl    Learning
-----  ------ ----  -------------------------------  -------------------------------  ------------
3     Enabled    100M/Full/Enabled        Link Down                Enabled
      MDI

DGS-1100-06/ME:5#
```

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 port settings.

```
DGS-1100-06/ME:5# show duld ports
Command: show duld ports

port  Admin State  Oper Status  Mode    Link Status    Discovery Time(Sec)
-----  -----------------  ----------------  --------  -----------------  ----------------------------
1     Disabled     Disabled     Normal  Unknown      5
2     Disabled     Disabled     Normal  Unknown      5
3     Disabled     Disabled     Normal  Unknown      5
4     Disabled     Disabled     Normal  Unknown      5
5     Disabled     Disabled     Normal  Unknown      5
6     Disabled     Disabled     Normal  Unknown      5


DGS-1100-06/ME: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] [enable | disable]
config loopdetect	interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]
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-1100-06/ME:5#enable loopdetect
Command: enable loopdetect


Success!
DGS-1100-06/ME:5#
```

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-1100-06/ME:5#disable loopdetect
Command: disable loopdetect


Success!
DGS-1100-06/ME:5#
```

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 | vlanbase]]* - Specifies the loopdetect mode to be portbase or vlanbase.
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-1100-06/ME:5#config loopdetect mode portbase
Command: config loopdetect mode portbase


Success!
DGS-1100-06/ME:5#
```

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] [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 the Switch:

```
DGS-1100-06/ME:5#config loopdetect ports all enable
Command: config loopdetect ports all enable
```

```
Success!
DGS-1100-06/ME:5#
```

config loopdetect

Purpose	To configure the loop back detection interval time and recover time on the Switch.
Syntax	**config loopdetect interval_time <value 1-32767> lbd_recover_time [0 | <value 60-1000000>]**
Description	The **config loopdetect** command configures the loop back detection interval time and recover time on the Switch.
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. 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-1100-06/ME:5#config loopdetect interval_time 500
Command: config loopdetect interval_time 500

Success!
DGS-1100-06/ME:5#
```

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-1100-06/ME:5#show loopdetect
Command: show loopdetect


 Loopdetect Global Settings


 ----------------------------------
Loopdetect Status     : Enabled
Loopdetect Mode       : Port-Base
```

```
Loopdetect Interval  : 100
Recover Time         : 60
DGS-1100-06/ME: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	<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: Client 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-1100-06/ME:5#config pppoe circuit_id_insertion state enable
Command: config pppoe circuit_id_insertion state enable
```

```
Success.

DGS-1100-06/ME:5#
```

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 <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	<*portlist*> – Specifies a list of 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 1~5 PPPoE circuit ID insertion function and use Host MAC:

```
DGS-1100-06/ME:5#config pppoe circuit_id_insertion ports 1-5 circuit_id
mac state enable
Command: config pppoe circuit_id_insertion ports 1-5 circuit_id mac
state enable

Success.

DGS-1100-06/ME:5#
```

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-1100-06/ME:5#show pppoe circuit_id_insertion
Command: show pppoe circuit_id_insertion

Status: Enabled

DGS-1100-06/ME:5#
```

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 {<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	*<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 2 to 5:

```
DGS-1100-06/ME:5#show pppoe circuit_id_insertion ports 2-5
Command: show pppoe circuit_id_insertion ports 2-5

Port State    Cirucit ID
---- -------- ------------------------------------
2    Enabled  Switch MAC
3    Enabled  Switch MAC
4    Enabled  Switch MAC
5    Enabled  Switch MAC

DGS-1100-06/ME:5#
```

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> <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>
enable snmp traps	
disable snmp traps	
show snmp traps	
enable snmp authenticate trap	
disable snmp authenticate trap	
config syslocation	<string 20>
config sysname	<string 20>
config syslogintimeout	<integer 3-30>
enable snmp	
disable snmp	
enable snmp fiber_port_link traps	
disable snmp fiber_port_link traps	
enable snmp LBD traps	
disable snmp LBD traps	
enable snmp port_security_violation traps	
disable snmp port_security_violation traps	
enable snmp system_device_bootup traps	
disable snmp system_device_bootup traps	
enable snmp twistedpair_port_link traps	
disable snmp twistedpair_port_link	

Command	Parameter
traps	

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-1100-06/ME:5#create snmp user dlink SW22 v3 MD5 1234 DES jklj22
Command: create snmp user dlink SW22 v3 MD5 1234 DES jklj22


Success!

DGS-1100-06/ME: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-1100-06/ME:5#delete snmp user dlink v3
Command: delete snmp user dlink v3


Success!
DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#
```

delete snmp view

Purpose	To remove an SNMP view entry previously created on the Switch.
Syntax	delete snmp view <view_name 32> <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. *<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 a previously configured SNMP view from the Switch:

```
DGS-1100-06/ME:5#delete snmp view dlink 1.3.6
Command: delete snmp view dlink 1.3.6

Success.

DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#create snmp community dlinkgroup dlink
Command: create snmp community dlinkgroup dlink

Success.

DGS-1100-06/ME: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 'dlink':

```
DGS-1100-06/ME:5#delete snmp community dlink
Command: delete snmp community dlink


Success!

DGS-1100-06/ME: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-1100-06/ME:5#show snmp community
```

```
Command: show snmp community

SNMP Community Table
(Maximum Entries : 10)

Community Name          User Name
------------------------ ------------
public                  ReadOnly
private                 ReadWrite

Total Entries: 2

DGS-1100-06/ME: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-1100-06/ME:5#config snmp engineID 12345678900
Command: config snmp engineID 12345678900

Success!

DGS-1100-06/ME:5#
```

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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#delete snmp group sg1 v3 auth_priv
Command: delete snmp group sg1 v3 auth_priv


Success!

DGS-1100-06/ME: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-1100-06/ME:5#show snmp groups
Command: show snmp groups

SNMP Group Table

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-1100-06/ME: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 configured SNMP global state on the Switch:

```
DGS-1100-06/ME:5#show snmp global state
Command: show snmp global state


SNMP Global State : Enable


DGS-1100-06/ME: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>] {[InterfaceName <string 20>]}
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. *InterfaceName* <*string 20*> − Specifies the interface name for v1 and v2.
Restrictions	Only Administrator and oper-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#delete snmp host 10.90.90.22
Command: delete snmp host 10.90.90.22

Success!
```

```
DGS-1100-06/ME: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 configured SNMP hosts on the Switch:

```
DGS-1100-06/ME: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-1100-06/ME: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>] {InterfaceName <string 20>}
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. *InterfaceName <string 20>* − Specifies the interface name of v1 and v2c.
Restrictions	Only Administrator and oper-level users can issue this command

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-1100-06/ME:5#create snmp v6host 3000::1 v3 noauth_nopriv dlink
Command: create snmp v6host 3000::1 v3 noauth_nopriv dlink


Success!

DGS-1100-06/ME: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 host entry:

```
DGS-1100-06/ME:5#delete snmp v6host 90.90.22
```

```
Command: delete snmp host 10.90.90.22

Success!

DGS-1100-06/ME:5#
```

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-1100-06/ME: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-1100-06/ME:5#
```

enable snmp traps

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

Example usage:

To enable SNMP trap support on the Switch:

```
DGS-1100-06/ME:5#enable snmp traps
```

```
Command: enable snmp traps

Success!

DGS-1100-06/ME:5#
```

disable snmp traps

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

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DGS-1100-06/ME:5#disable snmp traps
Command: disable snmp traps

Success!

DGS-1100-06/ME: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-1100-06/ME:5#show snmp traps
Command: show snmp traps


SNMP Traps                          : Enable
SNMP Authentication Traps           : Enable
System Device Bootup                : Enable
Fiber Port Link Up / Link Down      : Enable
Twisted Pair Port Link Up / Link Down : Enable
Port Security violation State       : Enable
Loopback detection State            : Enable
DGS-1100-06/ME:5#
```

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

Example usage:

To turn on SNMP authentication trap support:

```
DGS-1100-06/ME:5#enable snmp authenticate traps
Command: enable snmp authenticate traps

Success!

DGS-1100-06/ME:5#
```

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

Example usage:

To disable the SNMP authentication trap support:

```
DGS-1100-06/ME:5#disable snmp authenticate traps
Command: disable snmp authenticate traps

Success!

DGS-1100-06/ME:5#
```

config syslocation	
Purpose	To enter a description of the location of the Switch.
Syntax	config syslocation <string 20>
Description	The config syslocation command enters a description of the location of the Switch. A maximum of 20 characters can be used.
Parameters	*<string 20>* - A maximum of 20 characters is allowed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch location for 'HQ5F':

```
DGS-1100-06/ME:5#config syslocation HQ5F
Command: config syslocation HQ5F


Success.
DGS-1100-06/ME:5#
```

config sysname

Purpose	To define the name for the Switch.
Syntax	config sysname <string 20>
Description	The config sysname command defines the name of the Switch.
Parameters	*<string 20>* - A maximum of 20 characters is allowed.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the Switch name as '28ME':

```
DGS-1100-06/ME:5#config sysname 28ME
Command: config sysname 28ME


Success.
DGS-1100-06/ME:5#
```

config syslogintimeout

Purpose	To define the login timout for the Switch.
Syntax	config syslogintimeout <integer 3-30>
Description	The config syslogintimeout command defines the login timeout of the Switch.
Parameters	<integer 3-30> - Specifies the login timeout. The range is from 3-30 minutes.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the login timeout to 30 minutes:

```
DGS-1100-06/ME:5# config syslogintimeout 30
Command: config syslogintimeout 30


Success.
DGS-1100-06/ME: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-1100-06/ME:5#enable snmp
Command: enable snmp

Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable snmp
Command: disable snmp

Success!

DGS-1100-06/ME:5#
```

enable snmp fiber_port_link traps

Purpose	To enable SNMP fiber port link traps support on the Switch.
Syntax	enable snmp **fiber_port_link t**raps
Description	The enable snmp **fiber_port_link t**raps command enables SNMP fiber port link traps support on the Switch. After enables the SNMP fiber port link traps support, the Switch will send out a trap to the SNMP manage host when the fiber port is link up or link down.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To enable SNMP fiber port link traps support on the Switch:

```
DGS-1100-06/ME:5#enable snmp fiber_port_link traps
Command: enable snmp fiber_port_link traps
```

```
Success!

DGS-1100-06/ME:5#
```

disable snmp fiber_port_link traps

Purpose	To disable SNMP fiber port link traps.
Syntax	disable snmp **fiber_port_link t**raps
Description	The disable snmp **fiber_port_link t**raps command disables SNMP fiber port link traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command

Example usage:

To disable SNMP fiber port link traps support on the Switch:

```
DGS-1100-06/ME:5#disable snmp fiber_port_link traps
Command: disable snmp fiber_port_link traps

Success!

DGS-1100-06/ME:5#
```

enable snmp LBD traps

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

Example usage:

To enable SNMP LBD traps support on the Switch:

```
DGS-1100-06/ME:5#enable snmp LBD traps
Command: enable snmp LBD traps

Success!

DGS-1100-06/ME:5#
```

disable snmp LBD traps

Purpose	To disable SNMP LBD traps.
Syntax	disable snmp **LBD t**raps
Description	The disable snmp **LBD t**raps command disables SNMP LBD traps

	support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP LBD traps support on the Switch:

```
DGS-1100-06/ME:5#disable snmp LBD traps
Command: disable snmp LBD traps


Success!

DGS-1100-06/ME:5#
```

enable snmp port_security_violation traps

Purpose	To enable SNMP port security violation traps.
Syntax	enable snmp **port_security_violation t**raps
Description	The enable snmp **port_security_violation t**raps command enables SNMP port security violation traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable SNMP port security violation traps support on the Switch:

```
DGS-1100-06/ME:5#enable snmp port_security_violation traps
Command: enable snmp port_security_violation traps


Success!

DGS-1100-06/ME:5#
```

disable snmp port_security_violation traps

Purpose	To disable SNMP port security violation traps.
Syntax	disable snmp **port_security_violation t**raps
Description	The disable snmp **port_security_violation t**raps command disables SNMP port security violation traps on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable SNMP port security violation traps support on the Switch:

```
DGS-1100-06/ME:5#disable snmp port_security_violation traps
Command: disable snmp port_security_violation traps
```

```
Success!

DGS-1100-06/ME:5#
```

enable snmp system_device_bootup traps

Purpose	To enable SNMP system device bootup traps support on the Switch.
Syntax	enable snmp **system_device_bootup traps**
Description	The enable snmp **system_device_bootup traps** command enables SNMP system device bootup traps support on the Switch. After enables the SNMP system device bootup traps support, the Switch will send out a trap to the SNMP manage host when the device is power on.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the SNMP system device bootup traps on the Switch:

```
DGS-1100-06/ME:5#enable snmp system_device_bootup traps
Command: enable snmp system_device_bootup traps

Success!

DGS-1100-06/ME:5#
```

disable snmp system_device_bootup traps

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

Example usage:

To disable the SNMP system device bootup traps on the Switch:

```
DGS-1100-06/ME:5#disable snmp system_device_bootup traps
Command: disable snmp system_device_bootup traps

Success!

DGS-1100-06/ME:5#
```

enable snmp twistedpair_port_link traps

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

Example usage:

To enable the SNMP twisted pair ports link traps on the Switch:

```
DGS-1100-06/ME:5#enable snmp twistedpair_port_link traps
Command: enable snmp twistedpair_port_link traps


Success!

DGS-1100-06/ME:5#
```

disable snmp twistedpair_port_link traps

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

Example usage:

To disable the SNMP twisted pair ports link traps on the Switch:

```
DGS-1100-06/ME:5#disable snmp twistedpair_port_link traps
Command: disable snmp twistedpair_port_link traps


Success!

DGS-1100-06/ME:5#
```

10

DISCOVERY TRAP COMMANDS

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

Command	Parameter
enable discover trap	[ipaddr]
disable discover trap	
enable discover_trap_event DeviceBoot	
disable discover_trap_event DeviceBoot	
enable discover_trap_event FiberPort	
disable discover_trap_event FiberPort	
enable discover_trap_event IllegalLogin	
disable discover_trap_event IllegalLogin	
enable discover_trap_event LBD	
disable discover_trap_event LBD	
enable discover_trap_event PortSecurity	
disable discover_trap_event PortSecurity	
enable discover_trap_event TwistedPairPort	
disable discover_trap_event TwistedPairPort	

Command	Parameter
show discover_trap	

Each command is listed in detail, as follows:

enable discover_trap

Purpose	To enable the discovery trap from smartconsole support of the Switch.
Syntax	enable discover_trap [ipaddr]
Description	The enable discover_trap command enables discovery traps support on the Switch.
Parameters	[*ipaddr]* – Specifies the IP address to be trapped to.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery trap to IP 10.90.90.97:

```
DGS-1100-06/ME:5# enable discover_trap 10.90.90.97
Command: enable discover_trap 10.90.90.97


Success.
DGS-1100-06/ME:5#
```

disable discover_trap

Purpose	To disable the discovery trap from smartconsole support of the Switch.
Syntax	disable discover_trap
Description	The disable discover_trap command disables discovery traps support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery trap:

```
DGS-1100-06/ME:5# disable discover_trap
Command: disable discover_trap


Success.
DGS-1100-06/ME:5#
```

enable discover_trap_event DeviceBoot

Purpose	To enable the discovery device bootup trap from smartconsole

	support of the Switch.
Syntax	enable discover_trap_event DeviceBoot
Description	The enable discover_trap_event DeviceBoot command enables discovery device bootup trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery device boot trap:

```
DGS-1100-06/ME:5# enable discover_trap_event DeviceBoot
Command: enable discover_trap_event DeviceBoot


Success.
DGS-1100-06/ME:5#
```

disable discover_trap_event DeviceBoot

Purpose	To disable the discovery device bootup trap from smartconsole support of the Switch.
Syntax	disable discover_trap_event DeviceBoot
Description	The disable discover_trap_event DeviceBoot command disables discovery device bootup trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery device boot trap:

```
DGS-1100-06/ME:5# disable discover_trap_event DeviceBoot
Command: disable discover_trap_event DeviceBoot


Success.
DGS-1100-06/ME:5#
```

enable discover_trap_event FiberPort

Purpose	To enable the discovery fiber port trap from smartconsole support of the Switch.
Syntax	enable discover_trap_event FiberPort
Description	The enable discover_trap_event FiberPort command enables discovery fiber port trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery fiber port trap:

```
DGS-1100-06/ME:5# enable discover_trap_event FiberPort
Command: enable discover_trap_event FiberPort


Success.
DGS-1100-06/ME:5#
```

disable discover_trap_event FiberPort

Purpose	To disable the discovery fiber port trap from smartconsole support of the Switch.
Syntax	disable discover_trap_event FiberPort
Description	The disable discover_trap_event FiberPort command disables discovery fiber port trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery fiber port trap:

```
DGS-1100-06/ME:5# disable discover_trap_event FiberPort
Command: disable discover_trap_event FiberPort


Success.
DGS-1100-06/ME:5#
```

enable discover_trap_event IllegalLogin

Purpose	To enable the discovery illegal login trap from smartconsole support of the Switch.
Syntax	enable discover_trap_event IllegalLogin
Description	The enable discover_trap_event IllegalLogin command enables discovery illegal login trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery illegal login trap:

```
DGS-1100-06/ME:5# enable discover_trap_event IllegalLogin
Command: enable discover_trap_event IllegalLogin


Success.
DGS-1100-06/ME:5#
```

disable discover_trap_event IllegalLogin

Purpose	To disable the discovery illegal login trap from smartconsole support of the Switch.
Syntax	disable discover_trap_event IllegalLogin
Description	The disable discover_trap_event IllegalLogin command disables discovery illegal login trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery illegal login trap:

```
DGS-1100-06/ME:5# disable discover_trap_event IllegalLogin
Command: disable discover_trap_event IllegalLogin


Success.
DGS-1100-06/ME:5#
```

enable discover_trap_event LBD

Purpose	To enable the discovery loopback detection trap from smartconsole support of the Switch.
Syntax	enable discover_trap_event IllegalLogin
Description	The enable discover_trap_event IllegalLogin command enables discovery loopback detection trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery loopback detection trap:

```
DGS-1100-06/ME:5# enable discover_trap_event LBD
Command: enable discover_trap_event LBD


Success.
DGS-1100-06/ME:5#
```

disable discover_trap_event LBD

Purpose	To disable the discovery loopback detection trap from smartconsole support of the Switch.
Syntax	disable discover_trap_event LBD
Description	The disable discover_trap_event LBD command disables discovery loopback detection trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery loopback detection trap:

```
DGS-1100-06/ME:5# disable discover_trap_event LBD
Command: disable discover_trap_event LBD


Success.
DGS-1100-06/ME:5#
```

enable discover_trap_event PortSecurity

Purpose	To enable the discovery port security trap from smartconsole support of the Switch.
Syntax	enable discover_trap_event PortSecurity
Description	The enable discover_trap_event PortSecurity command enables discovery l port security trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery port security trap:

```
DGS-1100-06/ME:5# enable discover_trap_event PortSecurity
Command: enable discover_trap_event PortSecurity


Success.
DGS-1100-06/ME:5#
```

disable discover_trap_event PortSecurity

Purpose	To disable the discovery port security trap from smartconsole support of the Switch.
Syntax	disable discover_trap_event PortSecurity
Description	The disable discover_trap_event PortSecurity command disables discovery port security trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery port security trap:

```
DGS-1100-06/ME:5# disable discover_trap_event PortSecurity
Command: disable discover_trap_event PortSecurity


Success.
DGS-1100-06/ME:5#
```

enable discover_trap_event TwistedPairPort

Purpose	To enable the discovery twisted pair port trap from smartconsole support of the Switch.
Syntax	enable discover_trap_event TwistedPairPort
Description	The enable discover_trap_event TwistedPairPort command enables discovery twisted pair port trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable the discovery twisted pair port trap:

```
DGS-1100-06/ME:5# enable discover_trap_event TwistedPairPort
Command: enable discover_trap_event TwistedPairPort


Success.
DGS-1100-06/ME:5#
```

disable discover_trap_event TwistedPairPort

Purpose	To disable the discovery twisted pair port trap from smartconsole support of the Switch.
Syntax	disable discover_trap_event TwistedPairPort
Description	The disable discover_trap_event TwistedPairPort command disables discovery twisted pair port trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To disable the discovery twisted pair port trap:

```
DGS-1100-06/ME:5# disable discover_trap_event TwistedPairPort
Command: disable discover_trap_event TwistedPairPort


Success.
DGS-1100-06/ME:5#
```

show discover_trap

Purpose	To display the discovery trap information from smartconsole of the Switch.
Syntax	show discover_trap
Description	The show discover_trap command displays discovery trap information on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the discovery trap:

```
DGS-1100-06/ME:5# show discover_trap
Command: show discover_trap

Trap Settings for SmartConsole
------------------------------------------------------------
Trap Status                 : ENABLE
Destination IP              : 10.90.90.97
Device Bootup               : DISABLE
Illegal Login               : ENABLE
Fiber Port Event            : ENABLE
Twisted Pair Port Event     : ENABLE
Port Security Violation     : DISABLE
Loopback detection State: DISABLE
DGS-1100-06/ME:5#
```

11

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	[configuration [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [firmware [<ipaddr> | <ipv6_addr>] <string 64>]
upload	[[firmware [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [cfg_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> config_id <value 1-2>] | [log_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 **[configuration [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [firmware [<ipaddr> | <ipv6_addr>] <string 64>]**
Description	The download command downloads a firmware, boot, or switch configuration file from a TFTP server.
Parameters	*configuration* − 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* − Downloads and installs firmware on the Switch from a TFTP server. *<string 64>* − The DOS path and filename of the firmware file, up to 64 characters, on the TFTP server. For example, C:\31xx.had.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To download a firmware file:

```
DGS-1100-06/ME:5#download firmware 1.1.1.23 1\dgs_1100-06me.ros
Command: download firmware 1.1.1.23 1\ dgs_1100-06me.ros
01–Jan–2000 01:19:48 %COPY–I–FILECPY: Files Copy – source URL tftp://1.1.1.23 /1\
dgs_1100-06me.ros destination URL Unit all flash://image
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
```

```
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!01–Jan–2000 01:22:49 %COPY–W–TRAP:
The copy operation was completed successfully
!
3920460 bytes copied in 00:03:01 [hh:mm:ss]

DGS-1100-06/ME:5#
```

To download a configuration file:

```
DGS-1100-06/ME:5#download configuration 10.48.74.121 c:\cfg\setting.txt
Overwrite file [startup-config] ? [Yes/press any key for no]....
01-Jan-200003:19:46%COPY-I-FILECPY:FilesCopy-source URL tftp://10.48.74.121/1.txt
destination
URL flash://startup-config
Success.

Success.

.....01-Jan-2000 03:18:40 %COPY-N-TRAP: The copy operation was completed
successfully!
Copy: 267 bytes copied in 00:00:08 [hh:mm:ss]
DGS-1100-06/ME:5#
```

upload	
Purpose	To upload the current switch settings to a TFTP server.
Syntax	upload **[[firmware [<ipaddr> | <ipv6_addr>] <path_filename 64>] | [cfg_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64> config_id <value 1-2>] | [log_toTFTP [<ipaddr> | <ipv6_addr>] <path_filename 64>]]**
Description	The upload command uploads the Switch's current settings to a TFTP server.
Parameters	*firmware* − 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. *config_id <value 1-2>* − Specifies the config id which to be uploaded.

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

Example usage:

```
DGS-1100-06/ME:5#upload log_toTFTP 1.1.1.23 dgs_1100-06me.ros
Command: upload log_toTFTP 1.1.1.23 dgs_1100-06me.ros
01–Jan–2000 01:26:11 %COPY–I–FILECPY: Files Copy – source URL running–config destination URL tftp://1.1.1.23/1\running–config
…..01–Jan–2000 01:26:16 %COPY–W–TRAP: The copy operation was completed success fully!
158 bytes copied in 00:00:05 [hh:mm:ss]

DGS-1100-06/ME:5#
```

12

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> | 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>

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-1100-06/ME:5#enable dhcp_relay
Command: enable dhcp_relay

Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable dhcp_relay
Command: disable dhcp_relay

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config dhcp_relay add ipif System 10.6.150.49
Command: config dhcp_relay add ipif System 10.6.150.49

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config dhcp_relay delete ipif System 10.6.150.49
Command: config dhcp_relay delete ipif System 10.6.150.49


Success!

DGS-1100-06/ME:5#
```

config dhcp_relay

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	*hops <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-1100-06/ME:5#config dhcp_relay hops 12
Command: config dhcp_relay hops 12

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config dhcp_relay option_82 state disable
Command: config dhcp_relay option_82 state disable



Success!

DGS-1100-06/ME: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-1100-06/ME:5#show dhcp_relay
Command: show dhcp_relay



DHCP/BOOTP Relay Status             : Disabled
DHCP/BOOTP Hops Count Limit         : 4
DHCP/BOOTP Relay Time Threshold : 0
DHCP Relay Agent Information Option 82 State    : Disabled
DHCP Relay Agent Information Option 82 Check    : Disabled
DHCP Relay Agent Information Option 82 Policy   : Replace
DHCP Relay Agent Information Option 82 ID       : 00-B2-FD-DA-EE-EB

Interface   Server 1       Server 2       Server 3       Server 4
---------   ---------------  ---------------  ---------------  ---------------
DGS-1100-06/ME: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-1100-06/ME:5#enable dhcp_local_relay
Command: enable dhcp_local_relay


Success
DGS-1100-06/ME: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-1100-06/ME:5#disable dhcp_local_relay
Command: disable dhcp_local_relay


Success
DGS-1100-06/ME:5#
```

config dhcp_local_relay

Purpose	To specify which VLAN's the feature works on.
Syntax	**config dhcp_local_relay [vlan <vlan_name> | 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 <vlan_name>* – 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-1100-06/ME:5#config dhcp_local_relay vlan vlanid 10 state disable
Command: config dhcp_local_relay vlan vlanid 10 state disable
```

```
Success
DGS-1100-06/ME: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-1100-06/ME:5#show dhcp_local_relay
Command: show dhcp_local_relay

DHCP/BOOTP Local Relay Status  : Disabled
DHCP/BOOTP Local Relay VID List:

DGS-1100-06/ME: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-1100-06/ME:5#enable dhcpc6_relay
Command: enable dhcpc6_relay


Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable dhcpv6_relay
Command: disable dhcpv6_relay


Success!

DGS-1100-06/ME: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-1100-06/ME:5#show dhcpv6_relay ipif System
Command: show dhcpv6_relay ipif System

DHCPv6 Relay Global State : Enabled
DHCPv6 Hops Count Limit  : 4
-----------------------------------------------------------------
IP Interface                 : Syetem
Server Address               :

 Total Entries  : 0

DGS-1100-06/ME: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-1100-06/ME:5#config dhcpv6_relay add ipif System 3000::1
Command: config dhcpv6_relay add ipif System 3000::1


Success!

DGS-1100-06/ME: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-1100-06/ME:5#config dhcpv6_relay hop_count 3
Command: config dhcpv6_relay hop_count 3


Success!

DGS-1100-06/ME:5#
```

13

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 error ports	<portlist>
show utilization	[ports {<portlist>} | cpu | mem]
clear counters	
clear log	
show log	{[index <value 1-500> - <value 1-500>] | module <string 32> | severity [debug | informational | warning]}
save log	
enable syslog	
disable syslog	
show 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 1:

```
DGS-1100-06/ME:5#show packet ports 1
Command: show packet ports 1

Port Number : 1
Frame Size  Frame Counts  Frames/sec   Frame Type   Total    Total/sec
----------  ------------  ----------   ----------   -------  ---------
64          0             0            RX Bytes     0        0
65-127      0             0            RX Frames    0        0
128-255     0             0
256-511     0             0            TX Bytes     0        0
512-1023    0             0            TX Frames    0        0
1024-1518   0             0

Unicast RX    0           0
Multicast RX  0           0
Broadcast RX  0           0



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

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-1100-06/ME: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-1100-06/ME:5#
```

show utilization

Purpose	To display real-time port utilization statistics.
Syntax	show utilization **[ports {<portlist>} | cpu | mem]**
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. *mem* – Entering this parameter will display the current memory utilization of the Switch.
Restrictions	None.

To display the port 2 utilization statistics:

```
DGS-1100-06/ME:5#show utilization ports 2
Command: show utilization ports 2
 2   0     0     0


 Port TX/sec RX/sec Util
 ------ --------  ---------- ----
 2      0         0          0




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

DGS-1100-06/ME:5#
```

To display the cpu utilization statistics:

```
DGS-1100-06/ME:5#show utilization cpu
Command: show utilization cpu
Five Seconds - 6 %   One Minute - 6 %   Five Minutes - 6 %
Five Seconds - 7 %   One Minute - 6 %   Five Minutes - 6 %
Five Seconds - 7 %   One Minute - 6 %   Five Minutes - 6 %

CPU Utilization :
```

```
--------------------------------------------------------------------------------
Five Seconds - 7 %   One Minute - 6 %   Five Minutes - 6 %

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

DGS-1100-06/ME:5#
```

clear counters

Purpose	To clear the Switch's statistics counters.
Syntax	clear counters
Description	The clear counters command clears the counters used by the Switch to compile statistics.
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-1100-06/ME:5# clear counters
Command: clear counters

DGS-1100-06/ME: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-1100-06/ME:5#clear log
Command: clear log

Success!

DGS-1100-06/ME:5#
```

show log

Purpose	To display the Switch history log.
Syntax	show log {[index <value 1-500> - <value 1-500>] | module <string 32> | 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. *module <string 32>* − Specifies the module of log to be displayed. *severity [debug | informational | warning]* − Specifies the severity type to be displayed.
Restrictions	None.

Example usage:

To display the Switch history log:

```
DGS-1100-06/ME:5# show log
Command: show log

Index  Time                   Log Text
------- --------------------------- ----------------------------------------------------------------------------------
  1     Jan  1 00:00:18 2012:SYSTEM-2:System started up


DGS-1100-06/ME:5#
```

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-1100-06/ME:5# save log
Command: save log


Success!

DGS-1100-06/ME: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-1100-06/ME:5#enable syslog
Command: enable syslog

Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable syslog
Command: disable syslog

Success!

DGS-1100-06/ME:5#
```

show syslog

Purpose	To display the syslog protocol status.
Syntax	show syslog
Description	The show syslog command displays the syslog status (enabled or disabled).
Parameters	None.
Restrictions	None.

Example usage:

To display the current status of the syslog function:

```
DGS-1100-06/ME:5#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-1100-06/ME: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-1100-06/ME:5#create syslog host 1 ipaddress 1.1.2.1 severity all state enable
Command: create syslog host 1 ipaddress 1.1.2.1 severity all state enable

Success!
```

```
DGS-1100-06/ME: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 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 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-1100-06/ME:5#config syslog host 1 severity all facility local0
Command: config syslog host 1 severity all facility local0


Success.

DGS-1100-06/ME: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-1100-06/ME:5#delete syslog host all
Command: delete syslog host all

Success!

DGS-1100-06/ME: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-1100-06/ME:5#show syslog host
Command: show syslog host

Host ID  Host IP Address   Severity   Facility   UDP Port  Status
-------  ----------------  ---------  ---------  --------  ---------
1                1.1.2.1   All        Local0     514       Enabled
```

```
Total Entries : 1


DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#
```

14

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_name 32> <macaddr> port <port 1-6>
create multicast_fdb	<int 1-4094><macaddr>
config multicast_fdb	<integer 1-4094> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-600>
delete fdb	<vlan_name 32> <macaddr>
enable flood_fdb	
disable flood_fdb	
show flood_fdb	
clear flood_fdb	
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port 1-6> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
config multicast filter	<portlist> [forward | filter]
show multicast filter port_mode	
create auto_fdb	<ipaddr>
delete auto_fdb	<ipaddr>
show auto_fdb	{<ipaddr>}

Each command is listed in detail, as follows:

create fdb	
Purpose	To create a static entry in the unicast MAC address forwarding table (database)
Syntax	create fdb <vlan_name 32> <macaddr> port <port 1-6>
Description	The create fdb command creates a static entry in the Switch's unicast MAC address forwarding database.
Parameters	*<vlan_name 32>* − The name of the VLAN on which the MAC address resides. *<macaddr>* − The MAC address to be added to the forwarding table. *port <port 1-6>* − 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-1100-06/ME:5#create fdb default 00-00-00-00-01-02 port 2
Command: create fdb default 00-00-00-00-01-02 port 2

Success
DGS-1100-06/ME:5#
```

create multicast_fdb

Purpose	To create a static entry in the multicast MAC address forwarding table (database).
Syntax	create multicast_fdb <int 1-4094><macaddr>
Description	The create multicast_fdb command creates a static entry in the multicast MAC address forwarding table (database).
Parameters	*<integer 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-1100-06/ME:5#create multicast_fdb 1 00-00-00-01-02-03
Command: create multicast_fdb 1 00-00-00-01-02-03

Success.
DGS-1100-06/ME:5#
```

config multicast_fdb

Purpose	To configure the Switch's multicast MAC address forwarding database.
Syntax	config multicast_fdb <integer 1-4094> <macaddr> [add | delete] <portlist>
Description	The config multicast_fdb command configures the multicast MAC address forwarding table.
Parameters	*<integer 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-1100-06/ME:5#config multicast_fdb 1 00-00-00-01-02-03
Command: config multicast_fdb 1 00-00-00-01-02-03

Success.

DGS-1100-06/ME: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-1100-06/ME:5#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-1100-06/ME:5#
```

delete fdb

Purpose	To delete an entry in the Switch's forwarding database.
Syntax	delete fdb <vlan_name 32> <macaddr>
Description	The delete fdb command deletes an entry in the Switch's MAC address forwarding database.
Parameters	*<vlan_name 32>* − 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-1100-06/ME:5#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success
DGS-1100-06/ME: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.34
Parameters	None.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To enable FDB dynamic entries:

```
DGS-1100-06/ME:5#enable flood_fdb
Command: enable flood_fdb

Success.
DGS-1100-06/ME: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-1100-06/ME:5#disable flood_fdb
Command: disable flood_fdb

Success.
DGS-1100-06/ME: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	Only Administrator or operator-level users can issue this command.

Example usage:

To display FDB dynamic entries:

```
DGS-1100-06/ME:5#show flood_fdb
Command: show flood_fdb

Flooding FDB State : Enabled

VID   MAC Address      Port
----   -----------------      ----

DGS-1100-06/ME:5#
```

clear flood_fdb

Purpose	To clear the Switch's forwarding database of all dynamically learned MAC addresses.
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-1100-06/ME:5#clear flood_fdb
Command: clear flood_fdb

Success.
DGS-1100-06/ME:5#
```

show multicast_fdb

Purpose	To display the contents of the Switch's multicast forwarding database.
Syntax	show multicast_fdb {vlan <vlan_name 32> | 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 32>* − 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-1100-06/ME:5#show multicast_fdb
Command: show multicast_fdb

Static Multicast Table
----------------------

Total Mac Addresses displayed: 0

DGS-1100-06/ME:5#
```

show fdb

Purpose	To display the current unicast MAC address forwarding database.
Syntax	show fdb {port <port 1-28> | 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 1-28>* − 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-1100-06/ME: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-1100-06/ME:5#
```

To display the aging time:

```
DGS-1100-06/ME:5#show fdb aging_time
Command: show fdb aging_time

Unicast MAC Address Aging Time = 300 (seconds)

DGS-1100-06/ME:5#
```

config multicast filter

Purpose	To configure multicast filtering.
Syntax	**config multicast filter <portlist> [forward | filter]**
Description	The **config multicast filtering_mode** command enables filtering of multicast addresses.
Parameters	*<portlist>* - A port or range of ports to be configured. *forward* - Forwards unregistered multicast packets. *filter* - Filter unregistered multicast packets.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure multicast filtering

```
DGS-1100-06/ME:5#config multicast filter 3-5 forward
Command: config multicast filter 3-5 forward

Success!
DGS-1100-06/ME:5#
```

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-1100-06/ME:5# show multicast filter port_mode
Command: show multicast filter port_mode

 Port     Multicast Filtering Mode
------   --------------------------

   1   Filtering Unregistered Groups
   2   Filtering Unregistered Groups
```

```
   3   Filtering Unregistered Groups
   4   Forward Unregistered Groups
   5   Forward Unregistered Groups
   6   Forward Unregistered Groups
DGS-1100-06/ME:5#
```

create auto_fdb

Purpose	To create a static entry in the auto forwarding table (database).
Syntax	create auto_fdb <ipaddr>
Description	The create auto_fdb command creates a static entry in the multicast MAC address forwarding table (database).
Parameters	*<ipaddr>* − The IP address to be added to the auto forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To create auto forwarding table:

```
DGS-1100-06/ME:5#create auto_fdb 172.21.47.13
Command: create auto_fdb 172.21.47.13

Success.
DGS-1100-06/ME:5#
```

delete auto_fdb

Purpose	To delete a static entry in the auto forwarding table (database).
Syntax	delete auto_fdb <ipaddr>
Description	The delete auto_fdb command removes a static entry in the multicast MAC address forwarding table (database).
Parameters	*<ipaddr>* − The IP address to be deleted from the auto forwarding table.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To delete auto forwarding table:

```
DGS-1100-06/ME:5#delete auto_fdb 172.21.47.13
Command: delete auto_fdb 172.21.47.13

Success.
DGS-1100-06/ME:5#
```

show auto_fdb

Purpose	To display a static entry in the auto forwarding table (database).
Syntax	show auto_fdb {<ipaddr>}
Description	The show auto_fdb command displays a static entry in the multicast MAC address forwarding table (database).

Parameters	*<ipaddr>* − The IP address to be display from the auto forwarding table.
Restrictions	None.

Example usage:

To display auto forwarding table:

```
DGS-1100-06/ME:5#show auto_fdb
Command: show auto_fdb

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

Success.
DGS-1100-06/ME:5#
```

15

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] {[action [drop | shutdown] | countdown [0 | <minutes 5-30>] | broadcast | multicast | unicast | threshold <value 0-1024000> | time_interval <time_interval 5-30>]} [enable | disable]
show traffic control	{<portlist>}
config traffic trap	[storm_cleared | storm_occured | both | none]

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] {[action [drop | shutdown] | countdown [0 | <minutes 5-30>] | broadcast | multicast | unicast | threshold <value 0-1024000> | time_interval <time_interval 5-30>]} [enable | 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 [drop | shutdown]* − 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. *countdown [0 | <minutes 5-30>]* − Specifies the countdown time of traffic control. *storm_type* – The type of broadcast storm for which to configure the traffic control. The options are: • *broadcast* – Enables broadcast storm control only. • *multicast* – Enables broadcast and multicast storm control. • *unicast* – Enables broadcast and unicast 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. *<time_interval 5-30>* − Specifies the time interval of traffic control. *[enable | disable]* – Enables or disables the specified storm type.
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-1100-06/ME:5#config traffic control all multicast enable unicast disable br
oadcast enable threshold 65
Command: config traffic control all multicast enable unicast disable broadcast
enable threshold 65

Success.

DGS-1100-06/ME: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:

```
DGS-1100-06/ME:5# show traffic control
Command: show traffic control

Traffic Storm Control Trap : [None]

Port  Thres   Broadcast  Multicast  Unicast   Action   Count   Time
      hold    Storm      Storm      Storm              down    Interval
----  -------  ---------- ---------- ----------  --------  ---------  ---------
1     0        Disabled   Disabled   Disabled Drop     0        0
2     0        Disabled   Disabled   Disabled Drop     0        0
3     0        Disabled   Disabled   Disabled Drop     0        0
4     0        Disabled   Disabled   Disabled Drop     0        0
5     0        Disabled   Disabled   Disabled Drop     0        0
6     0        Disabled   Disabled   Disabled Drop     0        0


Total Entries : 6

DGS-1100-06/ME: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-1100-06/ME:5#config traffic trap storm_cleared
Command: config traffic trap storm_cleared

Success.

DGS-1100-06/ME:5#
```

16

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 64-1000000>] | tx_rate [no_limit | <value 64-1000000>]}
show bandwidth_control	{[<portlist> | all]}
config qos mode	[802.1p | dscp | portbased]
show qos mode	
config cos ipv6_tc_mapping	trafficclass <class_id 0-255> priority [high | highest | low | medium]
show cos ipv6_tc_mapping	{trafficclasee <class_id 0-255>}
delete cos ipv6_tc_mapping	d{trafficclasee <class_id 0-255>}
config scheduling_mechanism	[strict | wrr]
show scheduling_mechanism	
config dscp_mapping	dscp_value <value 0-63> priority [high | highest | low | medium]
show dscp_mapping	{dscp_value <value 0-63>}

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 64-1000000>] | tx_rate [no_limit | <value 64-1000000>]}
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 64–1000000*>] – Indicates a range between 64-1000000 kbps. *tx_rate* – Enables egress rate limiting.

	• *no_limit* – Indicates no limit is defined. • *<value 64–1000000>]* – Indicates a range between 64-1000000 kbps*.*
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure bandwidth control configuration:

```
DGS-1100-06/ME:5#config bandwidth_control all rx_rate no_limit tx_rate no_limit
Command: config bandwidth_control all rx_rate no_limit tx_rate no_limit

Success

DGS-1100-06/ME:5#
```

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-1100-06/ME:5#show bandwidth_control
Command: show bandwidth_control


Port  RX Rate   Tx Rate
----  -------   -------
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
6     no_limit  no_limit

Total entries : 10

DGS-1100-06/ME:5#
```

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-1100-06/ME:5# config qos mode portbased
Command: config qos mode portbased



Success

DGS-1100-06/ME: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-1100-06/ME:5# show qos mode
Command: show qos mode



Qos mode : portbase

DGS-1100-06/ME:5#
```

config cos ipv6_tc_mapping

Purpose	To configure the CoS IPv6 TC mapping method.
Syntax	config cos ipv6_tc_mapping trafficclass <class_id 0-255> priority [high | highest | low | medium]
Description	The config cos ipv6_tc_mapping command is used to configure the CoS IPv6 mapping method on the Switch.
Parameters	*<class_id 0-255>* - Specifies the IPv6 traffic class to be mapped. The range is 0 to 255. *priority [high* | *highest* | *low* | *medium]* - Specifies the priority of the ipv6 mapping priority queue.

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

Example usage:

To configure the CoS IPv6 mapping on the Switch:

```
DGS-1100-06/ME:5# config cos ipv6_tc_mapping trafficclass 10 priority high
Command: config cos ipv6_tc_mapping trafficclass 10 priority high



Success!

DGS-1100-06/ME:5#
```

show cos ipv6_tc_mapping

Purpose	To display the CoS IPv6 mapping method.
Syntax	show cos ipv6_tc_mapping {trafficclasee <class_id 0-255>}
Description	The show cos ipv6_tc_mapping command is used to display the CoS TC mapping method on the Switch.
Parameters	*<class_id 0-255>* - Specifies the IPv6 traffic class to be displayed. The range is 0 to 255.
Restrictions	None.

Example usage:

To display the CoS ipv6 mapping on the Switch:

```
DGS-1100-06/ME:5# show cos ipv6_tc_mapping trafficclass 10
Command: show cos ipv6_tc_mapping trafficclass 10

IPv6 Traffic TC           Priority
--------------------------------  ---------
10                         High



DGS-1100-06/ME:5#
```

delete cos ipv6_tc_mapping

Purpose	To remove the CoS IPv6 TC mapping method.
Syntax	delete cos ipv6_tc_mapping {trafficclasee <class_id 0-255>}
Description	The delete cos ipv6_tc_mapping command is used to delete the CoS IPv6 TC mapping method on the Switch.
Parameters	*<class_id 0-255>* - Specifies the IPv6 traffic class to be removed. The range is 0 to 255.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To delete the CoS ipv6 mapping on the Switch:

```
DGS-1100-06/ME:5# delete cos ipv6_tc_mapping trafficclass 10
Command: delete cos ipv6_tc_mapping trafficclass 10
```

```
Success!

DGS-1100-06/ME: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-1100-06/ME:5#config scheduling_mechanism strict
Command: config scheduling_mechanism strict

Success

DGS-1100-06/ME: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-1100-06/ME:5#show scheduling_mechanism
Command: show scheduling_mechanism

QOS Scheduling_mechanism

scheduling_mechanism  : Strict Priority

DGS-1100-06/ME:5#
```

config dscp_mapping

Purpose	To enable setting the DSCP User Priority
Syntax	config dscp_mapping dscp_value <value 0-63> priority [high | highest | low | medium]
Description	The config dscp_mapping command enables mapping the DSCP value (the priority) to a specific queue (the class_id).
Parameters	*<value 0-63>* –The selected value of priority. The value may be between 0 and 63. *[high | highest | low | medium]* – Specifies the priority to be mapped.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the DSCP mapping with value 10 and priority high:

```
DGS-1100-06/ME:5# config dscp_mapping dscp_value 10 priority high
Command: config dscp_mapping dscp_value 10 priority high


Success

DGS-1100-06/ME:5#
```

show dscp_mapping

Purpose	To display the setting of DSCP mapping.
Syntax	show dscp_mapping {dscp_value <value 0-63>}
Description	The show dscp_mapping command displays the mapping of DSCP value.
Parameters	*dscp_value <value 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 mapping with value 10:

```
DGS-1100-06/ME:5# show dscp_mapping dscp_value 10
Command: show dscp_mapping dscp_value 10


DSCP value Priority
---------- --------
10         High

DGS-1100-06/ME:5#
```

17

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 127>]}
delete rmon alarm	<alarm_index 1-65535>
create rmon collection stats	<stats_index 1-65535> port <ifindex> owner <owner_string 127>
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 127>}
delete rmon collection history	<hist_index 1-65535>
create rmon event	<event_index 1-65535> description <desc_string 127> {[log | owner <owner_string 127> | trap <community_string 127>]}
delete rmon event	<event_index 1-65535>
show rmon	

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-1100-06/ME:5#enable rmon
Command: enable rmon
```

```
Success!
DGS-1100-06/ME: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-1100-06/ME:5#disable rmon
Command: disable rmon


Success!
DGS-1100-06/ME: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 127>]}
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 127>* − 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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#delete rmon alarm 100
Command: delete rmon alarm 100

Success!
DGS-1100-06/ME: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 127>
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 127>* − 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-1100-06/ME:5#create rmon collection stats 100 port 2 owner dlink
Command: create rmon collection stats 100 port 2 owner dlink


Success!
DGS-1100-06/ME: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-1100-06/ME:5#delete rmon collection stats 2
Command: delete rmon collection stats 2

Success!
DGS-1100-06/ME: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 127>}
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-1100-06/ME:5#create rmon collection history 120 port 2 buckets 25
Command: create rmon collection history 120 port 2 buckets 25


Success!
DGS-1100-06/ME: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-1100-06/ME:5#delete rmon collection history 2
Command: delete rmon collection history 2

Success!
DGS-1100-06/ME: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 127> {[log | owner <owner_string 127> | trap <community_string 127>]}
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 127>* − Specifies the user-defined event description. *log* − Indicates that the event is a log entry. *owner <owner_string 127>* − Specifies the time that the event occurred. *trap <community_string 127>* − 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-1100-06/ME:5#create rmon event 125 description linkrmon owner
dlink
Command: create rmon event 125 description linkrmon owner dlink



Success!
DGS-1100-06/ME: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-1100-06/ME:5#delete rmon event 2
Command: delete rmon event 2

Success!
DGS-1100-06/ME:5#
```

show rmon

Purpose	To display remote monitoring (RMON) status for the SNMP function.
Syntax	show rmon
Description	The show rmon command displays remote monitoring (RMON) status for the SNMP function on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the RMON feature on the Switch:

```
DGS-1100-06/ME:5#show rmon
Command: show rmon

RMON is enabled
```

```
Success!
DGS-1100-06/ME:5#
```

18

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	
config mirror target	<short 1-28> [add | delete] source ports <portlist> [both | rx | tx]
show mirror	

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-1100-06/ME:5#enable mirror
Command: enable mirror

Success

DGS-1100-06/ME: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-1100-06/ME:5#disable mirror
Command: disable mirror

Success

DGS-1100-06/ME:5#
```

config mirror target

Purpose	To configure a mirror port − source port pair on the Switch.
Syntax	config mirror target <short 1-28> [add | delete] source ports <portlist> [both | rx | tx]
Description	The config mirror target 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	*target <short 1-28>* − 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. *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 add the mirroring ports:

```
DGS-1100-06/ME:5#config mirror target 4 add source ports 1-3 both
Command: config mirror target 4 add source ports 1-3 both

Success

DGS-1100-06/ME:5#
```

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

Example usage:

To display mirroring configuration:

```
DGS-1100-06/ME:5#show mirror
Command: show mirror

Port Mirror  is enabled
Target Port  : Fa0/4
Source Port : Fa0/1
Direction    : Both

Target Port  : Fa0/4
Source Port : Fa0/2
Direction    : Both

Target Port  : Fa0/4
Source Port : Fa0/3
Direction    : Both

DGS-1100-06/ME:5#
```

19

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	<string 20> {tag <int 2-4094>}
delete vlan	[<vlan_name 20> | vlanid <int 2-4094>]
config vlan	[<vlan_name 20> | vlanid <vlanid 1-4094>] [[add [tagged | untagged] | delete] <portlist>
config pvid	<int 1-4094> ports <portlist>
show vlan	{<int 1-4094>}
enable asymmetric_ vlan	
disable asymmetric_vlan	
show asymmetric_vlan	
enable management vlan	
disable management vlan	
config management vlan	<string 32>
show management vlan	
show port_vlan pvid	

Each command is listed in detail, as follows:

create vlan	
Purpose	To create a VLAN on the Switch.
Syntax	create vlan <string 20> {tag <int 2-4094>}
Description	The create vlan command creates a VLAN on the Switch.
Parameters	*<string 20>* − The name of the VLAN to be created. *tag <int 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-1100-06/ME:5#create vlan v1 tag 3
Command: create vlan v1 tag 3

Success
DGS-1100-06/ME:5#
```

delete vlan

Purpose	To delete a previously configured VLAN on the Switch.
Syntax	delete vlan [<vlan_name 20> | vlanid <int 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 <int 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 which VLAN ID is 2:

```
DGS-1100-06/ME:5#delete vlan vlanid 2
Command: delete vlan vlanid 2

Success
DGS-1100-06/ME: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 <vlanid 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 <vlanid 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 add ports 5 as tagged ports to the VLAN 3:

```
DGS-1100-06/ME:5# config vlan vlanid 3 add tagged 5
Command: config vlan vlanid 3 add tagged 5



Success
DGS-1100-06/ME:5#
```

config pvid

Purpose	To configure the pvid on the Switch.
Syntax	config pvid <int 1-4094> ports <portlist>
Description	The config pvid command configures the Group VLAN Registration Protocol on the Switch.
Parameters	<int 1-4094> − Specifies the PVID to be configured. <*portlist*> − A port or range of ports which user want to configure with.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the PVID on the Switch:

```
DGS-1100-06/ME:5#config pvid 1 ports 2
Command: config pvid 1 ports 2

Success.

DGS-1100-06/ME:5#
```

show vlan

Purpose	To display the current VLAN configuration on the Switch
Syntax	show vlan {<int 1-4094>}
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	<*int 1-4094*> − Specify the VLAN id to be displayed.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-1100-06/ME:5# show vlan
Command: show vlan

VID             : 1         VLAN NAME    : default
VLAN Type       : Static
Member Ports    : 1-6
```

```
Untagged Ports     : 1-6

DGS-1100-06/ME: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-1100-06/ME:5#enable asymmetric_vlan
Command: enable asymmetric_vlan

Success
DGS-1100-06/ME: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-1100-06/ME:5#disable asymmetric_vlan
Command: disable asymmetric_vlan

Success
DGS-1100-06/ME: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-1100-06/ME:5#show asymmetric_vlan
Command: show asymmetric_vlan

Asymmetric VLAN : Enable
DGS-1100-06/ME: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-1100-06/ME:5#enable management vlan
Command: enable management vlan


success
DGS-1100-06/ME: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-1100-06/ME:5#disable management vlan
Command: disable management vlan


success
DGS-1100-06/ME:5#
```

config management vlan

Purpose	To configure the management VLAN on the Switch.
Syntax	**config management vlan <string 32>**
Description	The **config management vlan** command configures the management VLAN on the Switch.
Parameters	*<string 32>* − Specifies the management VLAN name 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-1100-06/ME:5#config management vlan default
Command: config management vlan default



success
DGS-1100-06/ME:5#
```

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-1100-06/ME:5#show management vlan
Command: show management vlan



management vlan is enable

management vlan id : 1
management vlan name: default
DGS-1100-06/ME: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-1100-06/ME:5# show port_vlan pvid
Command: show port_vlan pvid

 Port    PVID
 -------------------
 01        1
 02        1
 03        1
 04        1
 05        1
 06        1
DGS-1100-06/ME:5#
```

20

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> | all]}
config qinq ports	[<portlist> | all] [role [nni | uni] | outer_tpid <hex 0x1-0xffff>]

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. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DGS-1100-06/ME:5#enable qinq
Command: enable qinq


Success!

DGS-1100-06/ME:5#
```

disable qinq	
Purpose	To disable the Q-in-Q mode.
Syntax	disable qinq
Description	The disable qinq command is used to disable the Q-in-Q mode. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared. All existing SP-VLANs will

	run as static 1Q VLANs. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DGS-1100-06/ME:5#disable qinq
Command: disable qinq


Success!

DGS-1100-06/ME:5#
```

show qinq

Purpose	To show global Q-in-Q and port Q-in-Q mode status.
Syntax	show qinq {ports [<portlist> | all]}
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. *all* - Specifies all ports to be displayed.
Restrictions	None.

Example usage:

To show the Q-in-Q status for ports 1 to 4:

```
DGS-1100-06/ME:5# show qinq ports 1-4
Command: show qinq ports 1-4

Port  Role  Outer TPID
------ ------  ----------------
1     UNI   0x8100
2     UNI   0x8100
3     UNI   0x8100
4     UNI   0x8100


DGS-1100-06/ME: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>]**
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.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure all ports as UNI port, set outer TPID to 0xfffe:

```
DGS-1100-06/ME:5# config qinq ports all outer_tpid 0xfffe role uni
Command: config qinq ports all outer_tpid 0xfffe role uni


Warning: The outer TPID will be globally applied to all ports!

Success!

DGS-1100-06/ME:5#
```

21

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	

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-1100-06/ME:5#config ipif System dhcpv6_client enable
Command: config ipif System dhcpv6_client enable
```

```
Success!

DGS-1100-06/ME: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-1100-06/ME:5# show ipif
Command: show ipif

IP Setting Mode                 : Static
IP Address                      : 10.90.90.90
Subnet Mask                     : 255.0.0.0
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-1100-06/ME
Ipv4 State                      : Enabled
IPv6 State                      : Enabled

DGS-1100-06/ME:5#
```

22

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	
show mac_notification ports	<portlist>

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-1100-06/ME:5#enable mac_notification
Command: enable mac_notification

Success.

DGS-1100-06/ME: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-1100-06/ME:5#disable mac_notification
Command: disable mac_notification

Success.

DGS-1100-06/ME: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-1100-06/ME:5#config mac_notification interval 1
Command: config mac_notification interval 1

Success.

DGS-1100-06/ME: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-1100-06/ME:5#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-1100-06/ME: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 Switch's MAC address table notification global settings.
Parameters	None.
Restrictions	None.

Example usage:

To view the Switch's MAC address table notification global settings:

```
DGS-1100-06/ME:5#show mac_notification
Command: show mac_notification


Global Mac Notification Settings

State          : Enabled
Interval       : 1
History Size   : 1
DGS-1100-06/ME: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 to display the Switch's MAC address table notification status settings.
Parameters	*<portlist>* – Specify a port or group of ports to be viewed. Entering this command without the parameter will display the MAC notification table for all ports.
Restrictions	None.

Example usage:

To display all port's MAC address table notification status settings:

```
DGS-1100-06/ME:5#show mac_notification ports 1-5
Command: show mac_notification ports 1-5
```

```
Port      MAC Address Table Notification State
----      ------------------------------------------------------
1                           Disabled
2                           Disabled
3                           Disabled
4                           Disabled
5                           Disabled

DGS-1100-06/ME:5#
```

23

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	{forward_mcrouter_only}
disable igmp_snooping	{forward_mcrouter_only}
show igmp_snooping	{vlan <vlan_name 20>}
config igmp_snooping	[vlan_name <string 20> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | leave_timer <sec 1-25> | fast_leave [enable | disable] | state [enable | disable]]
config igmp_snooping querier	[vlan_name <string 20> | vlanid <vidlist> | all] state [enable | disable] {querier_version [IGMPv2 | IGMPv3] | last_member_query_interval <sec 1-25> | max_response_time <sec 10-25> | query_interval <sec 60-600>}
config igmp_snooping querier_selection	[vlan_name <string 20> | vlanid <vidlist> | all] state [enable | disable]
config igmp_snooping robustness_variable	<integer 2-255>
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> [add | delete] [member_port <portlist> | source_port <portlist> | tag_member_port <portlist>] state [enable | disable] {replace_source_ip [none | <ipaddr>]}
delete igmp_snooping multicast_vlan	[<vlan_name 32> | all]
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add | delete] ipv4_range <ipaddr>
config router_ports	[vlan_name <string 20> | vlanid <vidlist> | all] [add | delete] <portlist>
config igmp access_authentication ports	[<portlist> | all] state [enable | disable]
show igmp access_authentication ports	[<portlist> | all]
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	<vlan_name 32>
show igmp_snooping	<vlan_name 32>

Command	Parameter
multicast_vlan_group	
show igmp_snooping group	{vlan <vlan_name 20>}
show igmp_snooping forwarding	[all | vlan_name <string 20> | vlanid <vidlist>]
show igmp_snooping host	{group <ipaddr> | ports <portlist> | vlan_name <string20>}
show igmp_snooping statistic counter	[vlan_name <string 20> | vlanid <vidlist> | ports <portlist> | all]
clear igmp_snooping statistic counter	
show router_port	{vlan <vlan_name 20> | static | dynamic}

Each command is listed in detail, as follows:

enable igmp_snooping	
Purpose	To enable IGMP snooping on the Switch.
Syntax	enable igmp_snooping {forward_mcrouter_only}
Description	The enable igmp_snooping command enables IGMP snooping on the Switch.
Parameters	*{forward_mcrouter_only}* – Enables the forward mcrouter only for IGMP Snooping on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DGS-1100-06/ME:5# enable igmp_snooping
Command: enable igmp_snooping

Success !
DGS-1100-06/ME:5#
```

disable igmp_snooping	
Purpose	To disable IGMP snooping on the Switch.
Syntax	disable igmp_snooping {forward_mcrouter_only}
Description	The disable igmp_snooping command disables IGMP snooping on the Switch.
Parameters	*{forward_mcrouter_only}* – Disables the forward mcrouter only for IGMP Snooping on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DGS-1100-06/ME:5# disable igmp_snooping
Command: disable igmp_snooping

Success !
DGS-1100-06/ME: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-1100-06/ME:5# show igmp_snooping vlan default
Command: show igmp_snooping vlan default

IGMP Snooping Global State : Enable
Forward Router Only        : Disable

Vlan Name                  : default
Host Timeout               : 260
Leave Timer                : 1
Router Timeout             : 125
Querier State              : Disable
Querier Router Behavior    : Non-Querier
Querier Version            : IGMPV2
State                      : Disable
Multicast Fast Leave       : Disable

DGS-1100-06/ME:5#
```

config igmp_snooping

Purpose	To configure IGMP snooping on the Switch.
Syntax	config igmp_snooping **[vlan_name <string 20> | vlanid <vidlist> | all] [host_timeout <sec 130-153025> | router_timeout <sec 60-600> | leave_timer <sec 1-25> | fast_leave [enable | disable] | state [enable | disable]]**
Description	The config igmp_snooping command configures IGMP snooping on the Switch.
Parameters	*vlan_name <string 20>* − 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. *leave_timer <sec 1-25>* − Leave timer. The default is 10 seconds. *fast_leave [enable | disable]* − Enables or disables the fast leave. *state [enable | disable]* − Enables or disables IGMP snooping for the specified VLAN.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-1100-06/ME:5# config igmp_snooping vlan_name default
host_timeout 250 state
enable
Command: config igmp_snooping vlan_name default host_timeout 250
state enable



Success !
DGS-1100-06/ME:5#
```

config igmp_snooping querier

Purpose	To configure IGMP snooping querier on the Switch.
Syntax	config igmp_snooping **querier [vlan_name <string 20> | vlanid <vidlist> | all] state [enable | disable] {querier_version [IGMPv2 | IGMPv3] | last_member_query_interval <sec 1-25> | max_response_time <sec 10-25> | query_interval <sec 60-600>}**
Description	The config igmp_snooping **querier** command enables IGMP snooping querier on a specific VLAN.
Parameters	*vlan_name <string 20>* − 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 [IGMPv2 | IGMPv3]* − Specifies the IGMP Querier version on the VLAN. *last_member_query_interval <sec 1-25>* − Specifies the last member query interval of IGMP. The range is from 1 to 25 seconds. *max_response_time <sec 10-25>* − Specifies the max response time of IGMP. The range is from 10 to 25 seconds. *query_interval <sec 60-600>* − Specifies the query interval of IGMP.

	The range is from 60 to 600 seconds.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping:

```
DGS-1100-06/ME:5# config igmp_snooping querier vlanid 2 state enable
last_member_query_interval 2
Command: config igmp_snooping querier vlanid 2 state enable
last_member_query_interval 2



Success !
DGS-1100-06/ME:5#
```

config igmp_snooping querier_selection

Purpose	To configure IGMP snooping querier selection on the Switch.
Syntax	config igmp_snooping **querier_selection [vlan_name <string 20> | vlanid <vidlist> | all] state [enable | disable]**
Description	The config igmp_snooping **querier_selection** command configures IGMP snooping querier selection on a specific VLAN.
Parameters	*vlan_name <string 20>* − 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.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping querier selection:

```
DGS-1100-06/ME:5#config igmp_snooping querier_selection vlanid 2
disable
Command: config igmp_snooping querier_selection vlanid 2 disable



Success !
DGS-1100-06/ME:5#
```

config igmp_snooping robustness_variable

Purpose	To configure IGMP snooping robustness variable on the Switch.
Syntax	config igmp_snooping **robustness_variable <integer 2-255>**
Description	The config igmp_snooping **robustness variable** command configures IGMP snooping robustness variable on the Switch.
Parameters	*<integer 2-255>* − The IGMP snooping robustness variable of IGMP snooping is to be configured.

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

Example usage:

To configure the igmp snooping robustness variable:

```
DGS-1100-06/ME:5#config igmp_snooping robustness_variable 10
Command: config igmp_snooping robustness_variable 10


Success !
DGS-1100-06/ME: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 32> <vlanid 2-4094>**
Description	The create igmp_snooping **multicast_vlan** command creates an IGMP snooping multicast VLAN on the Switch.
Parameters	*vlan <vlan_name 32>* − 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-1100-06/ME:5#create igmp_snooping multicast_vlan mvln2 5
Command: create igmp_snooping multicast_vlan mvln2 5


Success!
DGS-1100-06/ME:5#
```

config igmp_snooping multicast_vlan

Purpose	To configure IGMP snooping multicast VLAN on the Switch.
Syntax	config igmp_snooping **multicast_vlan <vlan_name 32> [add | delete] [member_port <portlist> | source_port <portlist> | tag_member_port <portlist>] state [enable | disable] {replace_source_ip [none | <ipaddr>]}**
Description	The config igmp_snooping **multicast_vlan** command enables IGMP snooping multicast VLAN on the Switch.
Parameters	*vlan <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] − 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>]* −
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure the igmp snooping multicast VLAN:

```
DGS-1100-06/ME:5#config igmp_snooping multicast_vlan default state enable
Command: config igmp_snooping multicast_vlan default state enable

Success!
DGS-1100-06/ME: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 32> | all]**
Description	The delete igmp_snooping **multicast_vlan** command removes IGMP snooping multicast VLAN on the Switch.
Parameters	*<vlan_name 32>* − Specify the multicast vlan name to be removed on the Switch. *all* − Specify all multicast vlan names to be removed on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To remove the igmp snooping multicast VLAN 'rd1':

```
DGS-1100-06/ME:5#delete igmp_snooping multicast_vlan rd1
Command: delete igmp_snooping multicast_vlan rd1


Success!
DGS-1100-06/ME: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 32> [add | delete] ipv4_range <ipaddr>**
Description	The config igmp_snooping **multicast_vlan_group** command specifies an IGMP snooping multicast VLAN group on the Switch.
Parameters	*vlan <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>.

	ipv4_range <ipaddr> − Specify the IPv4 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-1100-06/ME:5#config igmp_snooping multicast_vlan_group default add ipv4_range 10.90.90.99
Command: config igmp_snooping multicast_vlan_group default add ipv4_range 10.90.90.99

Success!
DGS-1100-06/ME:5#
```

config router_ports

Purpose	To configure ports as router ports.
Syntax	config router_ports **[vlan_name <string 20> | vlanid <vidlist> | 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>* − 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 delete the static router port:

```
DGS-1100-06/ME:5#config router_ports vlanid 2 delete 2
Command: config router_ports vlanid 2 delete 2


Success !
DGS-1100-06/ME: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-1100-06/ME:5#config igmp access_authentication ports all state
enable
Command: config igmp access_authentication ports all state enable



Success !
DGS-1100-06/ME: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-1100-06/ME:5#show igmp access_authentication ports all
Command: show igmp access_authentication ports all

Port  Authentication State
------ ----------------------------
1      Disabled
2      Disabled
3      Disabled
4      Disabled
5      Disabled
6      Disabled



DGS-1100-06/ME:5#
```

enable igmp_snooping multicast_vlan

Purpose	To enable IGMP snooping multicast VLAN on the Switch.
Syntax	enable igmp_snooping multicast_vlan
Description	The enable igmp_snooping multicast_vlan command enables IGMP snooping on the Switch.
Parameters	*multicast_vlan* − Enables the multicast VLAN for IGMP Snooping on the Switch.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To enable IGMP snooping multicast VLAN on the Switch:

```
DGS-1100-06/ME:5#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success !
DGS-1100-06/ME:5#
```

disable igmp_snooping multicast_vlan

Purpose	To disable IGMP snooping multicast VLAN on the Switch.
Syntax	disable igmp_snooping multicast_vlan
Description	The disable igmp_snooping multicast_vlan command disables IGMP snooping multicast VLAN on the Switch. IGMP snooping can be disabled only if IP multicast routing is not being used. Disabling IGMP snooping allows all IGMP and IP multicast traffic to flood within a given IP interface.
Parameters	*multicast_vlan* − Disables the multicast VLAN for IGMP Snooping on the Switch.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

TTo disable IGMP snooping multicast VLAN on the Switch:

```
DGS-1100-06/ME:5#disable igmp_snooping multicast_vlan
Command: disable igmp_snooping multicast_vlan


Success !
DGS-1100-06/ME:5#
```

show igmp_snooping multicast_vlan

Purpose	To show the current status of IGMP snooping multicast VLAN on the Switch.
Syntax	show igmp_snooping multicast_vlan **<vlan_name 32>**
Description	The show igmp_snooping command displays the current IGMP snooping configuration on the Switch.
Parameters	<*vlan_name 32*> − The name of the VLAN for which IGMP snooping

	configuration is to be displayed. Up to 32 characters can be used.
Restrictions	None.

Example usage:

To show igmp snooping multicast VLAN:

```
DGS-1100-06/ME:5#show igmp_snooping multicast_vlan vlan default
Command: show igmp_snooping multicast_vlan vlan default


 IGMP Snooping Global State      : Disable
 Multicast Router Only           : Disable
 Data Driven Learning Max Entries : 64

 VLAN Name                       : default
 Query Interval                  : 1
 Max Response Time               : 10
 Robustness Value                : 2
 Last Member Query Interval      : 1
 Querier State                   : Disable
 Querier Role                    : Non-Querier
 Querier Select                  : Disable
 Querier IP                      : 10.90.90.90
 Querier Expiry Time             : 0
 State                           : Enable
 Fast Leave                      : Disable
 Version                         : 3
 Data Driven Learning Aged Out   : Disable


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

show igmp_snooping multicast_vlan_group

Purpose	To show the current status of IGMP snooping multicast VLAN froup 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 configuration on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping configuration is to be displayed. Up to 32 characters can be used.
Restrictions	None.

Example usage:

To show igmp snooping multicast VLAN group:

```
DGS-1100-06/ME:5# show igmp_snooping multicast_vlan_group rd1
Command: show igmp_snooping multicast_vlan_group rd1

VID  Vlan Name                IP Range
```

```
----  -------------------------------  ----------------------------------------


DGS-1100-06/ME: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 20>}**
Description	The show igmp_snooping group command displays the current IGMP snooping group configuration on the Switch.
Parameters	*vlan <vlan_name 20>* − The name of the VLAN for which IGMP snooping group configuration information is to be displayed. Up to 20 characters can be used.
Restrictions	None.

Example usage:

To show igmp snooping group:

```
DGS-1100-06/ME:5#show igmp_snooping group vlan default
Command: show igmp_snooping group vlan default

Total Entries : 0

DGS-1100-06/ME:5#
Reports         : 1
Port Member     : 3,4

Total Entries    : 1

DGS-1100-06/ME:5#
```

show igmp_snooping forwarding

Purpose	To display the IGMP snooping forwarding table entries on the Switch.
Syntax	show igmp_snooping forwarding [all | **vlan_name <string 20> | vlanid <vidlist>]**
Description	The show igmp_snooping forwarding command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	*all* − Specifies all IGMP snooping forwarding table information to be displayed. *vlan_name <string 20>* − The name of the VLAN for which IGMP snooping forwarding table information is to be displayed. Up to 20 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-1100-06/ME:5#show igmp_snooping forwarding vlan_name default
Command: show igmp_snooping forwarding vlan_name 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-1100-06/ME:5#
```

show igmp_snooping host

Purpose	To display the IGMP snooping host table entries on the Switch.
Syntax	show igmp_snooping host {group <ipaddr> | ports <portlist> | vlan_name <string20>}
Description	The show igmp_snooping host command displays the current IGMP snooping forwarding table entries currently configured on the Switch.
Parameters	group <ipaddr> – Specifies the IGMP Snooping group IP address to be displayed. ports <portlist> – Specifies the IGMP Snooping ports to be displayed. vlan_name <string 20> – Specifies the VLAN name of IGMP Snooping to be displayed.
Restrictions	None.

Example usage:

To view the IGMP snooping host table on the Switch:

```
DGS-1100-06/ME:5#show igmp_snooping host
Command: show igmp_snooping host

VLAN ID   Group              Port No    IGMP Host
 ------    ----------------------  ---------    ------------



Total Entries : 0

DGS-1100-06/ME:5#
```

show igmp_snooping statistic counter

Purpose	To display the IGMP snooping statistic counter table entries on the Switch.
Syntax	show igmp_snooping statistic counter [vlan_name <string 20> | vlanid <vidlist> | ports <portlist> | all]

Description	The show igmp_snooping statistic counter command displays the current IGMP snooping statistic counter table entries currently configured on the Switch.
Parameters	*vlan_name <string 20>* – The name of the VLAN for which to view the IGMP snooping statistic counter configurations. *vlanid <vidlist>* – The id of the VLAN for which to view the IGMP snooping statistic counter configurations. *all* – Displays that all IGMP snooping which configured for all VLANs on the Switch. *ports <portlist>* – The ports of the VLAN for which to view the IGMP snooping statistic counter configurations.
Restrictions	None.

Example usage:

To view the IGMP snooping statistic counter table on the Switch:

```
DGS-1100-06/ME:5# show igmp_snooping statistic counter vlanid 1

Command: show igmp_snooping statistic counter vlanid 1


Snooping Statistics for VLAN 1
  General queries received : 0
  Group specific queries received : 0
 Group and source specific queries received : 0
  ASM reports received : 0
  SSM reports received : 0
  IS_INCLUDE messages received : 0
  IS_EXCLUDE messages received : 0
  TO_INCLUDE messages received : 0
  TO_EXCLUDE messages received : 0
  ALLOW messages received : 0
  Block messages received : 0
  Leave messages received : 0
  General queries transmitted : 0
  Group specific queries transmitted : 0
  ASM reports transmitted : 0
  SSM reports transmitted : 0
  Leaves transmitted : 0
  Packets dropped : 0

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

clear igmp_snooping statistic counter

Purpose	To clear the IGMP snooping statistic counter table entries on the Switch.
Syntax	clear igmp_snooping statistic counter
Description	The clear igmp_snooping statistic counter command clears the current IGMP snooping statistic counter table entries currently

	configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To clear the IGMP snooping statistic counter table on the Switch:

```
DGS-1100-06/ME:5# clear igmp_snooping statistics counter
Command: clear igmp_snooping statistics counter


Success !
DGS-1100-06/ME:5#
```

show router_port

Purpose	To display the currently configured router ports on the Switch.
Syntax	show router_port {vlan <vlan_name 20> | static | dynamic}
Description	The show router_port command displays the router ports currently configured on the Switch.
Parameters	*vlan <vlan_name 20>* − The name of the VLAN on which the router port resides. Up to 32 characters can be used. *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-1100-06/ME:5#show router_ports
Command: show router_ports

VLAN Name            : default
Static router port   :
Dynamic router port  :
Forbidden router port :

Total Entries : 1
DGS-1100-06/ME:5#
```

24

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	{forward_mcrouter only}
disable mld_snooping	{forward_mcrouter only}
config mld_snooping	[vlan_name <string 20> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-1530255> | leave_timer <sec 1-25> | router_timeout <sec 60-600> | state [enable | disable]}
config mld_snooping mrouter_ports	[vlan_name <string 20> | vlanid <vidlist> | all] [add | delete] <portlist>
config mld_snooping querier	[vlan_name <string 20> | 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>]
enable mld snooping multicast_vlan	
disable mld snooping multicast_vlan	
create mld snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
delete mld snooping multicast_vlan	[<vlan_name 32> | all]
config mld_snooping multicast_vlan	<vlan_name 32> [[add |delete] member_port <portlist>] replace_source_ipv6 <ipv6addr>] {state [enable | disable]}
config mld_snooping multicast_vlan_group	<vlan_name 32> [add |delete] ipv6_range <ipv6addr> <ipv6addr>
show mld snooping	[vlan_name <string 20> | vlanid <vidlist> | all]
show mld_snooping forwarding	[vlan_name <string 20> | vlanid <vidlist> | all]
show mld_snooping group	[vlan_name <string 20> | vlanid <vidlist> | all | ports <portlist>]
show mld_snooping mrouter_ports	[vlan_name <string 20> | vlanid <vidlist> | all] [dynamic | static]
show mld_snooping statistic counter	[vlan_name <string 20> | vlanid <vidlist> | all | ports <portlist>]
clear mld_snooping statistics counter	
show mld_snooping host	[vlan_name <string 20> | vlanid <vidlist> | all | ports <portlist> | group <ipv6_addr>]

Each command is listed in detail, as follows:

enable mld_snooping

Purpose	To enable MLD snooping on the Switch.
Syntax	enable mld snooping {forward_mcrouter only}
Description	The **enable** mld snooping command enables MLD snooping on the Switch.
Parameters	*forward_mcrouter only* – Enableds the forwarding multicast router only of MLD snooping.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To enable the MLD snooping:

```
DGS-1100-06/ME:5#enable mld_snooping
Command: enable mld_snooping


Success !
DGS-1100-06/ME:5#
```

disable mld_snooping

Purpose	To disable MLD snooping on the Switch.
Syntax	**disable** mld snooping {forward_mcrouter only}
Description	The **disable** mld snooping command disables MLD snooping on the Switch.
Parameters	*forward_mcrouter only* - Disables the forwarding multicast router only of MLD snooping.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To disable the MLD snooping:

```
DGS-1100-06/ME:5#disable mld_snooping
Command: disable mld_snooping


Success !
DGS-1100-06/ME:5#
```

config mld_snooping

Purpose	To configure mld snooping.
Syntax	**config mld_snooping [vlan_name <string 20> | vlanid <vidlist> | all] {fast_done [enable | disable] | host_timeout <sec 130-1530255> | leave_timer <sec 1-25> | router_timeout <sec 60-600> | state [enable | disable]}**
Description	The **config mld_snooping** command defines mld snooping on the VLAN.

Parameters	*vlan_name <string 20>* – 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 done to be enabled or disabled. *host_timeout <sec 130-1530255>* – 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. *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* – Allows the user to enable or disable MLD snooping for the specified VLAN.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure mld snooping:

```
DGS-1100-06/ME:5# config mld_snooping vlan_name default router_timeout
600 leave_timer 2 fast_done enable host_timeout 130 state enable
Command: config mld_snooping vlan_name default router_timeout 600
leave_timer 2 fast_done enable host_timeout 130 state enable



Success !
DGS-1100-06/ME:5#
```

config mld_snooping mrouter_ports

Purpose	To enable mld mrouter ports.
Syntax	**config mld_snooping mrouter_ports** [vlan_name **<string 20> | 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 20>* – 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 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-1100-06/ME:5#config mld_snooping mrouter_ports vlanid 1 add 3,5
Command: config mld_snooping mrouter_ports vlanid 1 add 3,5


Success !
DGS-1100-06/ME: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 20> | 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 20>* – 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 or operator–level users can issue this command.

Example usage:

To configure MLD snooping querier:

```
DGS-1100-06/ME:5#config mld_snooping querier vlan_name 2 last_listener_query_interval 1 query_interval 60
Command: config mld_snooping querier vlan_name 2 last_listener_query_interval 1 query_interval 60

Success!
DGS-1100-06/ME:5#
```

enable mld_snooping multicast_vlan

Purpose	To enable MLD snooping multicast VLAN on the Switch.
Syntax	enable mld snooping multicast_vlan
Description	The **enable** mld snooping multicast_vlan command enables MLD snooping multicast VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To enable the MLD snooping multicast VLAN:

```
DGS-1100-06/ME:5# enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan

Success.

DGS-1100-06/ME:5#
```

disable mld_snooping multicast_vlan

Purpose	To disable MLD snooping multicast VLAN on the Switch.
Syntax	**disable** mld snooping multicast_vlan
Description	The **disable** mld snooping multicast_vlan command disables MLD snooping multicast VLAN on the Switch.
Parameters	None.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To disable the MLD snooping multicast VLAN:

```
DGS-1100-06/ME:5#disable mld_snooping multicast_vlan
Command: disable mld_snooping multicast_vlan


Success !
```

```
DGS-1100-06/ME:5#
```

create mld_snooping multicast_vlan

Purpose	To create MLD snooping multicast VLAN on the Switch.
Syntax	**create** mld snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>
Description	The **create** mld snooping multicast_vlan command creates MLD snooping multicast VLAN on the Switch.
Parameters	*<vlan_name 32>* – Specifies the VLAN name of MLD snooping to be created. *<vlanid 2-4094>* – Specifies the VLAN id of MLD snooping to be created.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To create the MLD snooping multicast VLAN:

```
DGS-1100-06/ME:5# create mld_snooping multicast_vlan rd2 10
Command: create mld_snooping multicast_vlan rd2 10

Success.

DGS-1100-06/ME:5#
```

delete mld_snooping multicast_vlan

Purpose	To remove MLD snooping multicast VLAN on the Switch.
Syntax	**delete** mld snooping multicast_vlan [<vlan_name 32> | all]
Description	The **delete** mld snooping multicast_vlan command removes MLD snooping multicast VLAN on the Switch.
Parameters	*<vlan_name 32>* – Specifies the VLAN name of MLD snooping to be created. *all* – Specifies all MLD snooping multicast VLAN to be removed.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To remove the MLD snooping multicast VLAN:

```
DGS-1100-06/ME:5# delete mld_snooping multicast_vlan rd2
Command: delete mld_snooping multicast_vlan rd2

Success.

DGS-1100-06/ME:5#
```

config mld_snooping multicast_vlan

Purpose	To configure mld snooping multicast VLAN.
Syntax	**config mld_snooping multicast_vlan <vlan_name 32> [[add**

	|delete] member_port <portlist>] replace_source_ipv6 <ipv6addr>] {state [enable | disable]}
Description	The **config mld_snooping multicast_vlan** command defines mld snooping multicast VLAN on the VLAN.
Parameters	*vlan_name <vlan_name 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *[add | delete] member_port <portlist>* – Specifies the ports to be added or deleted of the vlan. *replace_source_ipv6 <ipv6addr>* – Specifies the IPv6 address to be configured. *state* – Allows the user to enable or disable MLD snooping multicast VLAN for the specified VLAN.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure mld snooping multicast VLAN:

```
DGS-1100-06/ME:5# config mld_snooping multicast_vlan default add member_port 1
Command: config mld_snooping multicast_vlan default add member_port 1

Success !
DGS-1100-06/ME:5#
```

config mld_snooping multicast_vlan_group

Purpose	To configure mld snooping multicast VLAN group.
Syntax	**config mld_snooping multicast_vlan_group <vlan_name 32> [add |delete] ipv6_range <ipv6addr> <ipv6addr>**
Description	The **config mld_snooping multicast_vlan_group** command defines mld snooping multicast VLAN group on the VLAN.
Parameters	*vlan_name <vlan_name 32>* – Specifies that the mld snooping applies only to this previously created VLAN. *[add | delete]* – Specifies the multicast VLAN group of MLD snooping to be added or deleted. *ipv6_range <ipv6addr> <ipv6addr>* – Specifies the IPv6 address range.
Restrictions	Only administrator or operator-level users can issue this command.

Example usage:

To configure mld snooping multicast VLAN group:

```
DGS-1100-06/ME:5# config mld_snooping multicast_vlan_group default add ipv6_range 2000::1 3000::1
Command: config mld_snooping multicast_vlan_group default add ipv6_range 2000::1 3000::1

Success !

DGS-1100-06/ME:5#
```

show mld snooping

Purpose	To display mld snooping settings on the Switch.
Syntax	show mld snooping **[vlan_name <string 20> | vlanid <vidlist> | 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_name <string 20>* – 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 MLD snooping which configured for all VLANs on the Switch.
Restrictions	None.

Example usage:

To show the MLD snooping:

```
DGS-1100-06/ME:5# show mld_snooping vlanid 1-3
Command: show mld_snooping vlanid 1-3


MLD Snooping Global State     : Enable

VLAN Name                     : default
Query Interval                : 125
Max Response Time             : 10
Robustness Value              : 2
Last Member Query Interval    : 2
Querier State                 : Disable
Querier Role                  : Non-Querier
Querier Select                : Enable
Querier IP                    :
Querier Expiry Time           : 0
State                         : Enable
Fast Leave                    : Enable
Version                       : 2


Total Entries : 1

DGS-1100-06/ME:5#
```

show mld_snooping forwarding

Purpose	To display mld snooping settings on the Switch.
Syntax	**show mld_snooping forwarding** [vlan_name <string 20> | 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 20>* – 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-1100-06/ME:5#show mld_snooping forwarding all
Command: show mld_snooping forwarding all


Total Entries : 0
DGS-1100-06/ME:5#
```

show mld_snooping group

Purpose	To display mld snooping group settings on the Switch.
Syntax	**show mld_snooping group [vlan_name <string 20> | 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 20>* – 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-1100-06/ME:5#show mld_snooping group all
Command: show mld_snooping group all


Total Entries : 0

DGS-1100-06/ME: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_name <string 20> | vlanid <vidlist> | 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 20>* – 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 configured MLD router posts.
Restrictions	None.

Example usage:

To show the MLD_snooping mrouterport:

```
DGS-1100-06/ME:5#show mld_snooping mrouter_ports vlanid 2 dynamic
Command: show mld_snooping mrouter_ports vlanid 2 dynamic

Total Entries : 0
DGS-1100-06/ME:5#
```

show mld_snooping statistic counter

Purpose	To display the MLD snooping statistics counters for MLD protocol packets that are transmitted or received by the switch since MLD snooping was enabled.
Syntax	**show mld_snooping statistic counter [vlan_name <string 20> | vlanid <vidlist> | all | ports <portlist>]**
Description	The **show mld_snooping statistic counter** command displays the MLD snooping statistics counters for MLD protocol packets that are transmitted or received by the switch since MLD snooping was enabled.
Parameters	*vlan_name <string 20>* – 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 a list of ports to be displayed.
Restrictions	None.

Example usage:

To show the MLD snooping statistic counte

```
DGS-1100-06/ME:5#show mld_snooping statistic counter all
```

```
Command: show mld_snooping statistic counter all

Total Entries : 0
DGS-1100-06/ME:5#
```

clear mld_snooping statistics counter

Purpose	To clear the mld snooping statistics counter on the Switch.
Syntax	**clear mld_snooping statistics counter**
Description	The **clear mld_snooping statistics counter** command is used to clear the mld snooping statistics counter on the Switch.
Parameters	None.
Restrictions	Only administrator or operator–level users can issue this command.

Example usage:

To clear MLD snooping statistics counter:

```
DGS-1100-06/ME:5#clear mld_snooping statistics counter
Command: clear mld_snooping statistics counter


Success !
DGS-1100-06/ME:5#
```

show mld_snooping host

Purpose	To display information of MLD snooping host on the Switch.
Syntax	**show mld_snooping host [vlan_name <string 20> | 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 20>* – 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-1100-06/ME:5#show mld_snooping host vlan_name default
Command: show mld_snooping host vlan_name default
```

```
Total Entries : 0


DGS-1100-06/ME:5#
```

25

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 32>
config mcast_filter_profile	[profile_id <integer 1-24> | profile_name <string 32>] [add | delete] <ipaddr>
config mcast_filter_profile ipv6	[profile_id <integer 1-24> | profile_name <string 32>] [add | delete] <ipv6addr>
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 32>] | access [permit | deny]}
show limited_multicast_addr ports	<portlist> {[ipv4 | ipv6]}
config max_mcast_group ports	<portlist> [ipv4 | ipv6] max_group <integer 1-256>
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 32>**
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 32>* - 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 IPv6 multicast filtering profile on the Switch:

```
DGS-1100-06/ME:5#create mcast_filter_profile ipv6 profile_id 1 profile_name
rd2
Command: create mcast_filter_profile ipv6 profile_id 1 profile_name rd2

Success.

DGS-1100-06/ME: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] <ipaddr>**
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. <*ipaddr*> – 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-1100-06/ME: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-1100-06/ME: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] <ipv6addr>**
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. *<ipv6addr>* – 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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#delete mcast_filter_profile ipv4 profile_name rd3
Command: delete mcast_filter_profile ipv4 profile_name rd3

Success.

DGS-1100-06/ME: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-1100-06/ME:5#show mcast_filter_profile
Command: show mcast_filter_profile

Type  Profile ID Profile Name
----- ---------- --------------------------------
v6    1          rd2
v6    4          rd4

[v6 Profiles]
ID  IPv6 Address Range
--  ----------------------------------------
4   ff0e:0000:0000:0000:0100:0000:0000:0020 ~
    ff0e:0000:0000:0000:0100:0000:0000:0022

DGS-1100-06/ME: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] [profile_id <integer 1-24> | profile_name <string 32>] | 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. *profile_id <integer 1-24>* – A profile ID to be added or deleted from a port. *profile_name <string 32>* – A profile name to be added or deleted from 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-1100-06/ME:5#config limited_multicast_addr ports 1,3 ipv6 add profile_id 1
Command: config limited_multicast_addr ports 1,3 ipv6 add profile_id 1

Success.

DGS-1100-06/ME: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-1100-06/ME:5#show limited_multicast_addr ports 1,3 ipv4
Command: show limited_multicast_addr ports 1,3 ipv4

Port Access     Profile ID List
---- ---------- ------------------------------------------------------------
1    (v4) Permit
3    (v4) Permit

DGS-1100-06/ME:5#
```

config max_mcast_group ports

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 ports** 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 1-32>* – Specifies the maximum number of multicast groups. The range is from 1 to 32.
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 10:

```
DGS-1100-06/ME:5#config max_mcast_group ports 1,3 ipv4 max_group 10
Command: config max_mcast_group ports 1,3 ipv4 max_group 10

Success.

DGS-1100-06/ME: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 to 3 settings:

```
DGS-1100-06/ME:5# show max_mcast_group ports 1-3 ipv6
Command: show max_mcast_group ports 1-3 ipv6

Port Max Group
---- ---------
1    (v6) 32
2    (v6) 32
3    (v6) 32

DGS-1100-06/ME:5#
```

26

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 init	port_based ports [<portlist> | all]
config 802.1x auth_protocol	[radius_eap | local]
config 802.1x reauth	port_based ports [<portlist> | all]
config radius add	<server_index 1-3> [<ipaddr> | <ipv6_addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}
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> | <ipv6_addr>] | 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 32>
delete 802.1x guest vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]
show 802.1x guest_vlan	
create 802.1x user	<username 15>

Command	Parameter
show 802.1x user	
delete 802.1x user	<username 15>
config 802.1x capability ports	[<portlist> | all] [authenticator | none]
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 switch wide:

```
DGS-1100-06/ME:5#enable 802.1x
Command: enable 802.1x


Success!
DGS-1100-06/ME: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 on the Switch:

```
DGS-1100-06/ME:5#disable 802.1x
Command: disable 802.1x
```

```
Success!
DGS-1100-06/ME: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 on the Switch:

```
DGS-1100-06/ME:5#show 802.1x
Command: show 802.1x

802.1X                    : Enable
Authentication Mode       : Port_base
Authentication Method     : Local

Success!
DGS-1100-06/ME: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 for port 1~5 for Port-based 802.1x:

```
DGS-1100-06/ME:5#show 802.1x auth_state ports 1-5
Command: show 802.1x auth_state ports 1-5

Port   Auth PAE State  Backend State  Port Status
------ --------------- -------------- ------------
1      ForceAuth       Success        Authorized
2      ForceAuth       Success        Authorized
3      ForceAuth       Success        Authorized
4      ForceAuth       Success        Authorized
5      ForceAuth       Success        Authorized
DGS-1100-06/ME: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-1100-06/ME:5#show 802.1x auth_configuration ports 2
Command: show 802.1x auth_configuration ports 2

Authentication Mode    : Port_base

Port number     : 2
Capability      : none
AdminCrlDir     : Both
OpenCrlDir      : Both
Port Control    : ForceAuthorized
QuietPeriod     : 60   sec
TxPeriod        : 30   sec
SuppTimeout     : 30   sec
ServerTimeout   : 30   sec
MaxReq          : 2    times
ReAuthPeriod    : 3600 sec
ReAuthenticate  : Disable

DGS-1100-06/ME: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 1-10> | 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 1-10>* – 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 for ports 1 – 3:

```
DGS-1100-06/ME:5#config 802.1x auth_parameter ports 1-3 direction both
Command: config 802.1x auth_parameter ports 1-3 direction both


Success!
DGS-1100-06/ME: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 or operator-level users can issue this command.

Example usage:

To initialize the authentication state machine of all ports:

```
DGS-1100-06/ME:5#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-1100-06/ME: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-1100-06/ME:5#config 802.1x auth_protocol local
Command: config 802.1x auth_protocol local

Success!

DGS-1100-06/ME: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 or operator-level users can issue this command.

Example usage:

To configure 802.1x reauthentication for ports 1-2:

```
DGS-1100-06/ME:5#config 802.1x reauth port_based ports 1-2
Command: config 802.1x reauth port_based ports 1-2

Success.

DGS-1100-06/ME: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> | <ipv6_addr>] [key <passwd 32>] {default | auth_port <udp_port_number 1-65535> | acct_port <udp_port_number 1-65535>}
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.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DGS-1100-06/ME:5#config radius add 1 10.48.47.11 key dlink default
Command: config radius add 1 10.48.47.11 key dlink default


Success!
DGS-1100-06/ME: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 communication settings:

```
DGS-1100-06/ME:5#config radius delete 1
Command: config radius delete 1

Success!
DGS-1100-06/ME: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> | <ipv6_addr>] | 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> | <ipv6_addr>]* – 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-1100-06/ME:5#config radius 1 ipaddress 10.48.47.11
Command: config radius 1 ipaddress 10.48.47.11


Success!
DGS-1100-06/ME: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 on the Switch:

```
DGS-1100-06/ME:5#show radius
Command: show radius

Index  Ip Address      Auth-Port  Acct-Port  Timeout  Retransmit  Key
                                              (secs)
-----  ----------------  ---------  ----------  ---------  ----------  ------
1      10.48.74.121      1812       1813       5          10          dlink

Total Entries : 1


Success!
DGS-1100-06/ME: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-1100-06/ME:5#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based


Success!
DGS-1100-06/ME:5#
```

create 802.1x guest_vlan

Purpose	Enables network access to a Guest VLAN.
Syntax	create 802.1x guest vlan **<vlan_name 32>**

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 32>* – 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-1100-06/ME:5#create 802.1x guest_vlan default
Command: create 802.1x guest_vlan default

Success.

DGS-1100-06/ME:5#
```

delete 802.1x guest_vlan

Purpose	Disables network access to a Guest VLAN.
Syntax	delete 802.1x guest vlan **<vlan_name 32>**
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	None.
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 a 802.1x Guest VLAN

```
DGS-1100-06/ME:5#delete 802.1x guest_vlan default
Command: delete 802.1x guest_vlan default

Success.

DGS-1100-06/ME: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-1100-06/ME:5#config 802.1x guest_vlan ports 1-3 state enable
Command: config 802.1x guest_vlan ports 1-3 state enable

Success.

DGS-1100-06/ME: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 information:

```
DGS-1100-06/ME: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-1100-06/ME:5#
```

create 802.1x user

Purpose	Enable network access to a 802.1x user.
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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#show 802.1x user
Command: show 802.1x user

Index      Username
---------- ---------------
 1         dlink

Total Entries: 1

Success!
DGS-1100-06/ME: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-1100-06/ME:5#delete 802.1x user dlink
Command: delete 802.1x user dlink


Success!
DGS-1100-06/ME: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 on the Switch:

```
DGS-1100-06/ME:5#config 802.1x capability ports all authenticator
Command: config 802.1x capability ports all authenticator


Success!
DGS-1100-06/ME:5#
```

config 802.1x fwd_pdu system

Purpose	Used to enable or disable the forwarding of EAPOL on the Switch.
Syntax	config 802.1x **fwd_pdu system [enable | disable]**
Description	Th config 802.1x **fwd_pdu system** is used to enable or disable the forwarding of EAPOL on the Switch.
Parameters	*[enable | disable]* – Enables or disables the forwarding of EAPOL PDU.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To configure forwarding of EAPOL PDU system state enable:

```
DGS-1100-06/ME:5# config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable


Success!
DGS-1100-06/ME:5#
```

show 802.1x fwd_pdu system status

Purpose	Used to display the forwarding of EAPOL status on the Switch.
Syntax	show 802.1x **fwd_pdu system status**
Description	Th show 802.1x **fwd_pdu system status** command displays the forwarding of EAPOL status on the Switch.
Parameters	None.
Restrictions	Only Administrator or operator–level users can issue this command.

Example usage:

To display the forwarding of EAPOL status on the Switch:

```
DGS-1100-06/ME:5# show 802.1x fwd_pdu system status
Command: show 802.1x fwd_pdu system status

PNAC control packet (eap) is forwarding....

Success!
DGS-1100-06/ME:5#
```

27

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>}

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-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#
```

28

PORT PRIORITY COMMANDS

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

Command	Parameter
config port_ priority	[<portlist> | all] priority [highest | low | medium | high]
show port_priority	{ all | <portlist> }

Each command is listed in detail, as follows:

config port_priority

Purpose	To configure port priority settings.
Syntax	config port_priority [<portlist> | all] priority [highest | low | medium | high]
Description	The config port_ priority command configures port priority settings for specific ports.
Parameters	*{all | <portlist>}* – Specifies all ports or range of ports to be configured. *[highest | low | medium | high]* – Specifies the priority of ports mapping priority queue.
Restrictions	Only administrator or operator-level users can issue this command

Example usage:

To configure port priority:

```
DGS-1100-06/ME:5# config port_priority all priority highest
Command: config port_priority all priority highest


Success

DGS-1100-06/ME:5#
```

show port_priority

Purpose	To display the current port priority configuration.
Syntax	show port_priority { all | <portlist> }
Description	The show port_ priority command displays port priority information for the Switch's ports.
Parameters	*{all | <portlist>}* – All ports or range of ports whose settings are to be displayed.
Restrictions	None.

Example usage:

To display the port priority configuration:

```
DGS-1100-06/ME:5# show port_priority all
Command: show port_priority all


Port  Priority
----  --------
1     Medium
2     Medium
3     Medium
4     Medium
5     Medium
6     Medium

DGS-1100-06/ME:5#
```

29

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-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#enable sntp
Command: enable sntp


Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable sntp
Command: disable sntp

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config time 09jan2012 15:50:50
Command: config time 09jan2012 15:50:50

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config time_zone operator + hour 2 minute 30
Command: config time_zone operator + hour 2 minute 30

Success!

DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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      : Disabled
Offset in Minutes                : 60
Annual From                      : 01 Jan 00:00
To                               : 01 Jan 00:00


DGS-1100-06/ME:5#
```

30

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	
show arpentry	{information | interface_name {system} | ip_address <ipaddr> | mac_address <macaddr> | summary}
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	*time <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-1100-06/ME:5#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-1100-06/ME: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-1100-06/ME:5#clear arptable
Command: clear arptable

Success.

DGS-1100-06/ME: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}**
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* – Displays the MAC address of ARP entry. *summary* – Displays the summary of ARP entry.
Restrictions	None.

Example usage:

To display all ARP entries information on the Switch:

```
DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#show arpentry aging_time
Command: show arpentry aging_time

ARP Aging Time = 30 (minutes)

DGS-1100-06/ME:5#
```

31

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 ipif	[system | all] [<ipv6_addr> | static | dynamic | all]
show ipv6 neighbor_cache ipif	[<ipif_name 12> | all] [ipv6address <ipv6_addr> | static | dynamic | all]
config ipv6 nd ns ipif	System retrans_time <integer 1-3600>
show ipv6 nd ipif System	
create ipv6route default	<ipv6addr>
delete ipv6route default	
show ipv6route	
enable ipif_ipv6_link_local_auto System	
disable ipif_ipv6_link_local_auto System	

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-1100-06/ME: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-1100-06/ME:5#
```

delete ipv6 neighbor_cache ipif

Purpose	Used to remove a static neighbor on an IPv6 interface.
Syntax	**delete ipv6 neighbor_cache ipif [System | all] [<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-1100-06/ME:5#delete ipv6 neighbor_cache 3ffc::1
Command: delete ipv6 neighbor_cache 3ffc::1


Success!

DGS-1100-06/ME:5#
```

show ipv6 neighbor_cache ipif

Purpose	Used to display the IPv6 neighbor cache.
Syntax	**show ipv6 neighbor_cache ipif [<ipif_name 12> | all] [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	*<ipif_name 12>* –The IPv6 interface name *all* - Displays all interfaces. *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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#config ipv6 nd ns ipif System retrans_time 100
Command: config ipv6 nd ns ipif System retrans_time 100

Success!

DGS-1100-06/ME:5#
```

show ipv6 nd ipif System

Purpose	Used to display information regarding neighbor detection on the switch.
Syntax	**show ipv6 nd ipif System**
Description	This **show ipv6 nd ipif System** 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-1100-06/ME:5# show ipv6 nd ipif System
Command: show ipv6 nd ipif System


Interface Name          : System
NS Retransmit Time      : 100(ms)
DGS-1100-06/ME: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-1100-06/ME:5#create ipv6route default 3ffc::1
Command: create ipv6route default 3ffc::1


Success.
DGS-1100-06/ME: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-1100-06/ME:5#delete ipv6route default
Command: delete ipv6route default


Success.
DGS-1100-06/ME: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-1100-06/ME:5# show ipv6route
Command: show ipv6route

IPv6 Prefix: ::/0                    Protocol: Static Metric: 1
Next Hop   : 2000::1                    IPIF    : System

Total Entries: 1

DGS-1100-06/ME: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-1100-06/ME:5#enable ipif_ipv6_link_local_auto System
Command: enable ipif_ipv6_link_local_auto System


Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System


Success!

DGS-1100-06/ME:5#
```

32

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_software_module	
show log	

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-1100-06/ME:5#config log_save_timing time_interval 30
Command: config log_save_timing time_interval 30

Success!

DGS-1100-06/ME:5#
```

show log_save_timing

Purpose	Used to show the login banner.
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-1100-06/ME:5#show log_save_timing
Command: show log_save_timing

Saving log method: time_interval
                   Interval : 300

DGS-1100-06/ME:5#
```

show log_software_module

Purpose	Used to show the login software module.
Syntax	**show log_software_module**
Description	This command allows display of the login software module on the Switch
Parameters	None.
Restrictions	None.

Usage Example:

To show the login software:

```
DGS-1100-06/ME:5# show log_software_module
Command: show log_software_module

CLI     SYSTEM

DGS-1100-06/ME:5#
```

show log	
Purpose	Used to show the login banner.
Syntax	**show log**
Description	This command allows display of the log.
Parameters	None.
Restrictions	None.

Usage Example:

To show the log on the Switch:

```
DGS-1100-06/ME:5# show log
Command: show log

Index   Time                  Log Text
------    --------------------      --------------------------------------------------------------------------
  2      Jan   1 00:01:13 2012:CLI-6:Successful login through console port( User: root )
  1      Jan  1 00:00:18 2012:SYSTEM-2:System started up


DGS-1100-06/ME:5#
```

33

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
?	
show command_history	
dir	

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-1100-06/ME:5#?
Command: ?


?
cable diagnostic port
clear arptable
clear counters
clear ethernet_oam ports
clear flood_fdb
clear igmp_snooping statistics counter
clear log
clear mld_snooping statistics counter
config 802.1x auth_mode ports
config 802.1x auth_parameter ports
config 802.1x auth_protocol
config 802.1x capability ports
config 802.1x fwd_pdu system
config 802.1x guest_vlan ports
config 802.1x init port_based ports
config 802.1x reauth port_based ports
config account
config admin local_enable
config arp_aging time
CTRL+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-1100-06/ME:5#show command_history
Command: show command_history

?
show log
show log_save_timing
show log_save_timing

DGS-1100-06/ME:5#
```

dir	
Purpose	To display all commands.
Syntax	dir
Description	The dir command displays all commands.
Parameters	None.
Restrictions	None.

Example usage:

To display all of the commands:

```
DGS-1100-06/ME:5# dir
Available commands:
?             cable         clear         config

create        delete        disable       download

enable        logout        ping          ping6

reboot        reload        reset         save

show          upload
DGS-1100-06/ME:5#
```

34

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>| ipv6address <ipv6addr>] protocol radius {port <int 1-65535> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	[<ipaddr> | ipv6address <ipv6addr>] protocol radius {port <int 1-65535> | key [<string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
delete authen server_host	[<ipaddr> | ipv6address <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> | ipv6address <ipv6addr>] protocol radius
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
enable admin	
config admin local_enable	

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-1100-06/ME:5#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity


Success.

DGS-1100-06/ME: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-1100-06/ME:5#config authen_login method_list_name Trinity method radius local
Command: config authen_login method_list_name Trinity method radius local


Success.

DGS-1100-06/ME: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-1100-06/ME:5#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DGS-1100-06/ME: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-1100-06/ME:5# show authen_login all
Command: show authen_login all


Method List Name  Priority  Method Name      Comment
------------------------- ---------- --------------------  ------------------
default                   1          local                 Keyword

Trinity                   1          none                  Keyword

DGS-1100-06/ME: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-1100-06/ME:5#create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.

DGS-1100-06/ME: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-1100-06/ME:5#config authen_enable method_list_name Trinity method
radius local
Command: config authen_enable method_list_name Trinity method  radius local

Success.

DGS-1100-06/ME: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-1100-06/ME:5#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit


Success.

DGS-1100-06/ME: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-1100-06/ME:5#show authen_enable all
Command: show authen_enable all


Method List Name  Priority  Method Name   Comment
----------------------    --------    ------------------    ------------------
default                 1         local              Keyword

DGS-1100-06/ME: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-1100-06/ME:5#enable authen_policy
Command: enable authen_policy

Success.

DGS-1100-06/ME: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-1100-06/ME:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-1100-06/ME: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-1100-06/ME:5#show authen_policy
Command: show authen_policy

Authentication Policy : Disabled

DGS-1100-06/ME: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-1100-06/ME:5#config authen application http login default
Command: config authen application http login default


Success.

DGS-1100-06/ME: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-1100-06/ME:5#show authen application
Command: show authen application


Application  Login Method List   Enable Method List
-----------  -------------------- ------------------
Console      default              default
Telnet       default              default
HTTP         default              default

DGS-1100-06/ME: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-1100-06/ME:5#config authen parameter attempt 10
Command: config authen parameter attempt 10


Success.

DGS-1100-06/ME: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-1100-06/ME:5#show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 10

DGS-1100-06/ME:5#
```

create authen server_host

Purpose	To create an authentication server host.
Syntax	create authen server_host [<ipaddr>| ipv6address <ipv6addr>] protocol radius {port <int 1-65535> | key [<string 254> | none] | 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. *ipv6address <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> | none]* – The authentication key to be shared with a configured RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*. *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-1100-06/ME: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

Key is empty for RADIUS.

Success.

DGS-1100-06/ME:5#
```

config authen server_host

Purpose	To configure a user-defined authentication server host.
Syntax	config authen server_host [<ipaddr> | ipv6address <ipv6addr>] protocol radius {port <int 1-65535> | key [<string 254> | none] | 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. *ipv6address<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> | none]* – The authentication key to be shared with a configured RADIUS server only. The value is a string of up to 254 alphanumeric characters, or *none*. *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-1100-06/ME: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-1100-06/ME:5#
```

delete authen server_host

Purpose	To delete a user-defined authentication server host.
Syntax	delete authen server_host [<ipaddr> | ipv6address <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. *ipv6address <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-1100-06/ME:5#delete authen server_host 10.1.1.121 protocol radius
Command: delete authen server_host 10.1.1.121 protocol radius


Success.

DGS-1100-06/ME: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-1100-06/ME:5# show authen server_host
Command: show authen server_host

IP Address: 10.1.1.121
   Protocol: radius
       Port: 4321
    Timeout: 12
Retransmit: 4
        Key:

Total Entries : 1

DGS-1100-06/ME: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-1100-06/ME:5#create authen server_group dlinkgroup
Command: create authen server_group dlinkgroup


Success.

DGS-1100-06/ME: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> | ipv6address <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. *ipv6address <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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#delete authen server_group dlinkgroup
Command: delete authen server_group dlinkgroup

Success.

DGS-1100-06/ME: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-1100-06/ME:5# show authen server_group
Command: show authen server_group

(1) Group Name: linkgroup

  (No servers in this group)


(2) Group Name: radius

  IP Address: 3000::
    Protocol: radius

  IP Address: 10.1.1.121
    Protocol: radius


Total Entries : 2

DGS-1100-06/ME: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-1100-06/ME:5#enable admin
Command: enable admin

Success!
DGS-1100-06/ME:5#
```

config admin local_enable

Purpose	To configure the local_enable password for administrator level privileges.
Syntax	config admin local_enable
Description	The config admin local_enable command changes the locally enabled password for the **local_enable admin** command. When a user chooses the '*local_enable*' method to promote user level privileges to administrator privileges, the user is prompted to enter the password configured here. After entering the config admin local_enable command, the user is prompted to enter the old password, then a new password in a string of no more than 15 alphanumeric characters, and finally prompted to enter the new password again for confirmation. See the example below.
Parameters	None.
Restrictions	Only administrator-level users can issue this command.

Example usage:

To configure the password for the 'local_enable' authentication method:

```
DGS-1100-06/ME:5#config admin local_enable
Command: config admin local_enable

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

DGS-1100-06/ME:5#
```

35

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-1100-06/ME:5# config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable


Success!

DGS-1100-06/ME: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-1100-06/ME:5# config power_saving mode port hibernation enable
Command: config power_saving mode port hibernation enable


Success!

DGS-1100-06/ME: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-1100-06/ME:5# show power_saving hibernation
Command: show power_saving hibernation

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

Time Range
-------------------------------
time_range_1:
time_range_2:

Port : All Port

DGS-1100-06/ME:5#
```

36

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 1-10>
config lldp tx_delay	<sec 1-8192>
config lldp notification_interval	<sec 5-3600>
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 [all | eapol | gvrp | lacp | stp][disable | enable]
config lldp ports	[<portlist>|all] dot1_tlv_vlan_name [vlan <vlan_name 32> | vlanid <vidlist>] [disable | enable]
show lldp mgt_addr	{ipv4 <ipaddr> | ipv6 <ipv6addr>}
show lldp statistics	{ports <portlist>}

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-1100-06/ME:5#enable lldp
Command: enable lldp

Success!

DGS-1100-06/ME: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-1100-06/ME:5#disable lldp
Command: disable lldp

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config lldp message_tx_interval 10
Command: config lldp message_tx_interval 10

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config lldp message_tx_hold_multiplier 2
Command: config lldp message_tx_hold_multiplier 2

Success!

DGS-1100-06/ME:5#
```

config lldp reinit_delay

Purpose	To define the lldp reinint–delay on the switch.
Syntax	**config lldp reinit_delay <sec 1-10>**
Description	The **lldp reinit_delay** *seconds* command specifies the minimum time an LLDP port will wait before reinitializing LLDP transmission.
Parameters	*<sec 1-10>* – 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-1100-06/ME:5#config lldp reinit_delay 1
Command: config lldp reinit_delay 1

Success!

DGS-1100-06/ME: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-1100-06/ME:5#config lldp tx_delay 1
Command: config lldp tx_delay 1


Success!

DGS-1100-06/ME:5#
```

config lldp notification_interval

Purpose	To configure the timer of the notification interval for sending notifications to configured SNMP trap receiver(s).
Syntax	**config lldp notification_interval <sec 5-3600>**
Description	The **config lldp notification_interval** command globally changes the interval between successive LLDP change notifications generated by the switch.
Parameters	*<sec 5-3600>* – The range is from 5 second to 3600 seconds. The default setting is 5 seconds.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To change the notification interval:

```
DGS-1100-06/ME:5#config lldp notification_interval 10
Command: config lldp notification_interval 10


Success!

DGS-1100-06/ME: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-1100-06/ME:5# show lldp
Command: show lldp

LLDP System Information
   Chassis Id Subtype      : MAC Address
   Chassis Id              : 00-AE-B7-21-22-62
   System Name             :
   System Description      : DGS-1100-06/ME        1.00.011
   System Capabilities     : Bridge

LLDP Configurations
   LLDP Status             : Enable
   Message Tx Interval     : 10
   Message Tx Hold Multiplier: 2
   ReInit Delay            : 1
   Tx Delay                : 1
   Notification Interval   : 5

DGS-1100-06/ME: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-1100-06/ME:5#show lldp ports 1

Port ID                 : 1
--------------------------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Disable
Advertised TLVs Option  :
   Port Description                                  Disable
   Port Description                                  Disable
   Port Description                                  Disable
   Port Description                                  Disable
   Enabled Management Address
     (NONE)
   Port VLAN ID                                      Disable
   Enabled Port_and_Protocol_VLAN_ID
     (None)
   Enabled VLAN Name
     (None)
   Enabled Protocol_Identity
     (None)
   MAC/PHY Configuration/Status                      Disable
   Power Via MDI                                     Disable
   Link Aggregation                                  Disable
   Maximum Frame Size                                Disable

DGS-1100-06/ME: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-1100-06/ME: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                  : Slot0/1
Port ID Desctiption      : Ethernet Interface


DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#config lldp ports 1-3 notification enable
Command: config lldp ports 1-3 notification enable


Success!

DGS-1100-06/ME: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-1100-06/ME:5#config lldp ports 2 admin_status disable
Command: config lldp ports 2 admin_status disable


Success!

DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#config lldp ports 1 basic_tlvs all enable
Command: config lldp ports 1 basic_tlvs all enable


Success!

DGS-1100-06/ME: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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#config lldp ports all dot1_tlv_pvid disable
Command: config lldp ports all dot1_tlv_pvid disable


Success!

DGS-1100-06/ME: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 [all | eapol | gvrp | lacp | stp][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 values are: eapol, gvrp, lacp, stp or all.
Restrictions	Only Administrator or operator-level users can issue this command.

Example usage:

To configure LLDP ports configuration status:

```
DGS-1100-06/ME:5#config lldp ports all dot1_tlv_protocol_identity eapol enable
Command: config lldp ports all dot1_tlv_protocol_identity eapol enable


Success!

DGS-1100-06/ME: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 32> | vlanid <vidlist>] [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 32>* –The name of the VLAN to be configured. *dot1_tlv_vlan_name* − Defines if the advertisement is enabled or disabled.

	vlanid <vidlist> –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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5#show lldp mgt_addr
Command: show lldp mgt_addr

Address : 1
--------------------------------------------------------------------------------
   Subtype                  : IPv6
   Address                  : fe80::2c8:e7ff:fe88:5c95
   IF Type                  : ifIndex
   OID                      : 1.3.6.1.2.1.2.2.1.1
   Advertising Ports        : (NONE)


Total Address : 1

DGS-1100-06/ME: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 15:

```
DGS-1100-06/ME:5#show lldp statistics ports 15
Command: show lldp statistics ports 15

Port ID : 15
-----------------------------------------------
lldpStatsTxPortFramesTotal                : 0
lldpStatsRxPortFramesDiscardedTotal  : 0
lldpStatsRxPortFramesErrors               : 0
lldpStatsRxPortFramesTotal                : 0
lldpStatsRxPortTLVsDiscardedTotal     : 0
lldpStatsRxPortTLVsUnrecognizedTotal : 0
lldpStatsRxPortAgeoutsTotal               : 0

DGS-1100-06/ME:5#
```

37

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-1100-06/ME:5#config traffic_segmentation 1-3 forward_list 5
Command: config traffic_segmentation 1-3 forward_list 5

Success.

DGS-1100-06/ME: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-1100-06/ME:5# show traffic_segmentation
Command: show traffic_segmentation


Port  Forward Portlist
----  -------------------------------------------------
1     5
2     5
3     5
4     1-6
5     1-6
6     1-6


DGS-1100-06/ME:5#
```

38

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 1-4294967295> | 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 <portlist>}
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-1100-06/ME:5# config ethernet_oam ports 1 mode passive
Command: config ethernet_oam ports 1 mode passive


Success!

DGS-1100-06/ME: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-1100-06/ME:5# config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable


Success!

DGS-1100-06/ME: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 1-4294967295> | 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 1-4294967295>* – 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-1100-06/ME: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-1100-06/ME: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 1-4294967295> | 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 1-4294967295>* – 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-1100-06/ME: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-1100-06/ME: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 1-4294967295> | 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 1-4294967295>* – 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-1100-06/ME: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-1100-06/ME: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 1-4294967295> | 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 1-4294967295>* – 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-1100-06/ME: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-1100-06/ME: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-1100-06/ME:5# config ethernet_oam ports 1 remote_loopback start
Command: config ethernet_oam ports 1 remote_loopback start


Success!

DGS-1100-06/ME: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-1100-06/ME:5# config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process



Success!

DGS-1100-06/ME: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 1:

```
DGS-1100-06/ME:5# show ethernet_oam ports 1 status
Command: show ethernet_oam ports 1 status


Port 1
Local Client
-------------------------------------------------------------
 OAM                    : Enabled
 Mode                   : Passive
 Max OAMPDU             : 1518 Bytes
 Remote Loopback        : Support
 Unidirection           : Not Supported
 Link Monitoring        : Support
 Variable Request       : Support
 PDU Revision           : 0
 Operation Status       : Disabled
 Loopback Status        : No Loopback


DGS-1100-06/ME:5#
```

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 2:

```
DGS-1100-06/ME:5# show ethernet_oam ports 2 configuration
Command: show ethernet_oam ports 2 configuration


Port 2
------------------------------------------------------------
  OAM                    : Disabled
  Mode                   : Active
  Critical Event          : Enabled
  Remote Loopback OAMPDU      : Not Processed

Symbol Error
  Notify State           : Enabled
  Window                 : 625000000 milliseconds
  Threshold              : 1 Errored Symbol

Frame Error
  Notify State           : Enabled
  Window                 : 10 milliseconds
  Threshold              : 1 Errored Frame

Frame Period Error
  Notify State           : Enabled
Window                   : 10000000 Frames
  Threshold              : 1 Errored Frame

Frame Seconds Error
  Notify State           : Enabled
  Window                 : 100 milliseconds
  Threshold              : 1 Errored Seconds


DGS-1100-06/ME:5#
```

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-1100-06/ME: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-1100-06/ME: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 <portlist>}**
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 <portlist>* – Specifies an index range to display.
Restrictions	None.

Example usage:

To show Ethernet OAM event log on port 1:

```
DGS-1100-06/ME:5# show ethernet_oam ports 1 event_log
Command: show ethernet_oam ports 1 event_log


Port 1
--------------------------------------------------------------------------
Event Listing
Index Type                                  Location     Time Stamp
----- ----------------------------------- ------------  ---------------------

Local Event Statistics
  Error Symbol Event                    : 0
  Error Frame Event                     : 0
  Error Frame Period Event              : 0
  Errored Frame Seconds Event           : 0
 Critical Event                        : 0
Remote Event Statistics
  Error Symbol Event                    : 0
  Error Frame Event                     : 0
  Error Frame Period Event              : 0
  Errored Frame Seconds Event           : 0
  Critical Event                        : 0

DGS-1100-06/ME: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-1100-06/ME:5# clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics


Success!

DGS-1100-06/ME:5#
```

39

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.
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-1100-06/ME:5#config safeguard_engine state enable
Command: config safeguard_engine state enable


Success!
DGS-1100-06/ME: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-1100-06/ME:5#show safeguard_engine
Command: show safeguard_engine


Safe Guard : Enabled
DGS-1100-06/ME:5#
```