D-Link
Building Networks for People

CLI Reference Manual

Product Model: DGS-3700 Series

Layer 2 Managed Gigabit Ethernet Switch

Release 1.00

July 2009 P/N 651GS3712015G

Table of Contents

1 INTRODUCTION

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

This manual provides a reference for all of the commands contained in the CLI. Configuration and management of the Switch via the Web-based management agent is discussed in the User Manual.

This manual provides a reference for all of the commands contained in the CLI for the DGS-3700-12 and DGS-3700-12G. Examples present in this manual may refer to either member of this series and may show different port counts, but are universal to this series of switches, unless otherwise stated. Configuration and management of the Switch via the Web-based management agent is discussed in the User Guide.

NOTE: For the remainder of this manual, the DGS-3700-12, DGS-3700-12G, switches will be referred to as simply the Switch or the DGS-3700 Series.

Accessing the Switch via the Serial Port

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

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

A computer running a terminal emulation program capable of emulating a VT-100 terminal and a serial port configured as above is then connected to the Switch's serial port via an RS-232 DB-9 cable.

With the serial port properly connected to a management computer, the following screen should be visible. If this screen does not appear, try pressing Ctrl+r to refresh the console screen.

```
                    DGS-3700-12G Gigabit Ethernet Switch
                          Command Line Interface

                              Firmware: Build 1.00.B042
                    Copyright(C) 2009 D-Link Corporation. All rights reserved.

UserName:
```

Figure 1-1. Initial CLI screen

There is no initial username or password. Just press the **Enter** key twice to display the CLI input cursor – **DGS-3700-12:5#**. This is the command line where all commands are input.

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. Users can change the default Switch IP address to meet the specification of your networking address scheme.

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

```
Boot Procedure                                                  V1.00.B002
-------------------------------------------------------------------------

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

 MAC Address   : 00-01-02-03-04-00
 H/W Version   :

 Please Wait, Loading V1.00.B035 Runtime Image .........  100 %


 UART init .............................................  100 %
 Device Discovery ......................................  100 %
 Configuration init ....................................  \_
```

Figure 1-2. Boot screen

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

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

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

1. Starting at the command line prompt, enter the commands **config ipif System ipaddress xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**. Where the **x**'s represent the IP address to be assigned to the IP interface named **System** and the **y**'s represent the corresponding subnet mask.
2. Alternatively, 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-3700-12:5#config ipif System ipaddress 10.24.73.21/255.0.0.0
Command: config ipif System ipaddress 10.73.21.21/8

Success.

DGS-3700-12:5#
```

Figure 1-3. Assigning an IP Address screen

In the above example, the Switch was assigned an IP address of 10.24.73.21 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 CONSOLE CLI

The DGS-3700 Series supports a console management interface that allows the user to connect to the Switch's management agent via a serial port and a terminal or a computer running a terminal emulation program. The console can also be used over the network using the TCP/IP Telnet protocol. The console program can be used to configure the Switch to use an SNMP-based network management software over the network.

This chapter describes how to use the console interface to access the Switch, change its settings, and monitor its operation.

***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 will be loaded.

Connecting to the Switch

The console interface is used by connecting the Switch to a VT100-compatible terminal or a computer running an ordinary terminal emulator program (e.g., the **HyperTerminal** program included with the Windows operating system) using an RS-232C serial cable. Your terminal parameters will need to be set to:

- **VT-100 compatible**
- **115200 baud**
- **8 data bits**
- **No parity**
- **One stop bit**
- **No flow control**

Users can also access the same functions over a Telnet interface. Once users have set an IP address for your Switch, users can use a Telnet program (in VT-100 compatible terminal mode) to access and control the Switch. All of the screens are identical, whether accessed from the console port or from a Telnet interface.

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

```
                    DGS-3700-12G Gigabit Ethernet Switch
                          Command Line Interface

                              Firmware: Build 1.00.B035
                    Copyright(C) 2009 D-Link Corporation. All rights reserved.

UserName:
```

Figure 2-1. Initial Console screen after logging in

Commands are entered at the command prompt, **DGS-3700-12:5#**.

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

```
?
cable_diag ports
cfm linktrace
cfm loopback
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear ethernet_oam ports
clear fdb
clear historical_counters ports
clear igmp_snooping data_driven_group
clear igmp_snooping statistic counter
clear log
clear mac_based_access_control auth_mac
clear mld_snooping data_driven_group
clear mld_snooping statistic counter
clear port_security_entry
clear vlan_counter statistics

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

Figure 2-2. The ? Command

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

```
DGS-3700-12:5#config account
Command: config account
Next possible completions:
<username>

DGS-3700-12:5#
```

Figure 2-3. Example Command Parameter Help

In this case, the command **config account** was entered with the parameter **<username>**. The CLI will then prompt users to enter the **<username>** with the message, **Next possible completions:**. Every command in the CLI has this feature, and complex commands have several layers of parameter prompting.

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

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

```
 DGS-3700-12:5#config account
Command: config account
Next possible completions:
<username>

DGS-3700-12:5#config account
Command: config account
Next possible completions:
<username>

DGS-3700-12:5#
```

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

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

command (**config account**) at the command prompt. Now the appropriate username can be entered and the **config account** command re-executed.

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

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

```
 DGS-3700-12:5#the
Available commands:
..                  ?                   cable_diag          cfm
clear               config              create              delete
disable             download            enable              login
logout              ping                ping6               reboot
reconfig            reset               save                show
upload

DGS-3700-12:5#
```

Figure 2-5. The Next Available Commands Prompt

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, if users enter the **show** command with no additional parameters, the CLI will then display all of the possible next parameters.

```
DGS-3700-12:5#show
Command: show
Next possible completions:
802.1p              802.1x              access_profile      account
accounting          acct_client         address_binding     arpentry
attack_log          auth_client         auth_diagnostics
auth_session_statistics                 auth_statistics     authen
authen_enable       authen_login        authen_policy       autoconfig
bandwidth_control   bpdu_tunnel         cfm                 command_history
config              cpu                 current_config      ddm
device_status       dhcp_relay          dot1v_protocol_group
dscp                error               ethernet_oam        external_alarm
fdb                 filter              firmware            flow_meter
greeting_message    gvrp                historical_counter
historical_utilization                  hol_prevention      igmp_snooping
ipif                ipif_ipv6_link_local_auto               iproute
ipv6                ipv6route           jumbo_frame         lacp_port
limited_multicast_addr                  link_aggregation    lldp
local_loopback      log                 log_save_timing     loopdetect
mac_based_access_control                mac_based_access_control_local
mac_based_vlan      mac_notification    max_mcast_group
mcast_filter_profile                    mgmt_pkt_priority   mirror
mld_snooping        multicast           multicast_fdb       out_band_ipif
packet              port                port_security
port_security_entry                     port_vlan           ports
pvid                qinq                radius              router_ports
rspan               safeguard_engine    scheduling
scheduling_mechanism                    serial_port         session
sflow               sim                 snmp                sntp
sred                ssh                 ssl                 stp
subnet_vlan         switch              syslog              system_severity
time                time_range          traffic
traffic_segmentation                    trusted_host        utilization
vlan                vlan_counter        vlan_precedence     vlan_translation
wac

DGS-3700-12:5#
```

Figure 2-6. Next possible completions: Show Command

In the above example, all of the possible next parameters for the **show** command are displayed. At the next command prompt, 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 console interface 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	**config ipif <ipif_name 12> [{ipaddress <network_address> |vlan <vlan_name 32> |state [enable |disable]}(1)| bootp |dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable| disable]] |ipv4 state [enable | disable]]**
Description	In the above syntax example, users must supply an IP interface name in the <ipif_name 12> space, a VLAN name in the <vlan_name 32> space, and the network address in the <network_address> space. Do not type the angle brackets.
Example Command	**config ipif Engineering ipaddress 10.24.22.5/255.0.0.0 vlan Design state enable**

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

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

{braces}	
Purpose	Encloses an optional value or set of optional arguments.
Syntax	**reset {[config |system]} {force_agree}**
Description	In the above syntax example, users have the option to specify **config** or **system**. It is not necessary to specify either optional value, however the effect of the system reset is dependent on which, if any, value is specified. Therefore, with this example there are three possible outcomes of performing a system reset. See the following chapter, Basic Commands for more details about the reset command. Do not type the braces.
Example command	**reset config**

(parentheses)	
Purpose	Indicates at least one or more of the values or arguments in the preceding syntax enclosed by braces must be specified.
Syntax	**config dhcp_relay {hops <value 1-16> | time <sec 0-65535>}(1)**
Description	In the above syntax example, users have the option to specify hopsor time orboth of them. The "(1)" following the set of bracesindicates at least one argument or valuewithin the braces must be specified. Do not type the parentheses.
Example command	**config dhcp_relay hops 3**

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.
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 will display 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	Parameters
create account	[admin | operator | user] <username 15>
config account	<username> {encrypt [plain_text| sha_1] <password>}
show account	
delete account	[<username>]
enable password encryption	
disable password encryption	
show session	
show switch	
show device_status	
show serial_port	
config serial_port	{ baud_rate [9600|19200|38400|115200] | auto_logout [never|2_minutes|5_minutes|10_minutes|15_minutes]}(1)
enable clipaging	
disable clipaging	
enable telnet	<tcp_port_number 1-65535>
disable telnet	
enable web	<tcp_port_number 1-65535>
disable web	
save	{[config <config_id 1-2> | log | all]}
reboot	
reboot	{force_agree}
reset	{[config |system]} {force_agree}
reset	{[config force_agree | system force_agree]}
login	
logout	

Each command is listed, in detail, in the following sections.

create account

Purpose	Used to create user accounts.
Syntax	**create account [admin | operator | user] <username 15>**
Description	This command is used to create user accounts that consist of a username of 1 to 15 characters and a password of 0 to 15 characters. Up to 8 user accounts can be created.
Parameters	[admin | operator | user] <username 15>
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.

Example usage:

To create an administrator-level user account with the username "dlink".

```
DGS-3700-12:5#create account admin dlink
Command: create account admin dlink

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

DGS-3700-12:5#
```

NOTICE: In case of lost passwords or password corruption, please refer to the "Password Recovery Command List" section in this manual, and the "Password Recovery Procedure" will guide you through the steps necessary to resolve this issue.

config account

Purpose	Used to configure user accounts
Syntax	**config account <username> {encrypt [plain_text| sha_1] <password>}**
Description	When the password information is not specified in the command, the system will prompt the user to input the password interactively. For this case, the user can only input the plain text password. If the password is present in the command, the user can select to input the password in the plain text form or in the encrypted form. The encryption algorithm is based on SHA-1.
Parameters	*<username>* – Name of the account. The account must already be defined. *plain_text* – Select to specify the password in plain text form. *sha_1* – Select to specify the password in the SHA-1 encrypted form. *password* – The password for the user account. The length for of password in plain-text form and in encrypted form are different. For the plain-text form, passwords must have a minimum of 0 character and can have a maximum of 15 characters. For the encrypted form password, the length is fixed to 35 bytes long. The assword is case-sensitive.
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.

Example usage:

To configure the user password of "dlink" account:

```
DGS-3700-12:5#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-3700-12:5#
```

show account

Purpose	Used to display user accounts.
Syntax	**show account**
Description	This command is used to display all user accounts created on the Switch. Up to 8 user accounts can exist at one time.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the accounts that have been created:

```
DGS-3700-12:5#show account
Command: show account

Current Accounts:
Username         Access Level
---------------  ------------
dlink             Admin

Total Entries: 1

DGS-3700-12:5#
```

delete account

Purpose	Used to delete an existing user account.
Syntax	**delete account <username>**
Description	This command is used to delete an existing account.
Parameters	*<username>* – Name of the user who will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user account “System”:

```
DGS-3700-12:5#delete account System
Command: delete account System

Success.

DGS-3700-12:5#
```

enable password encryption

Purpose	Used to enable password encryption.
Syntax	**enable password encryption**
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form when it is stored in the configuration file. When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plain text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It can not be reverted to the plain text.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable password encryption:

```
DGS-3700-12:5#enable password encryption
Command: enable password encryption

Success.

DGS-3700-12:5#
```

disable password encryption

Purpose	Used to disable password encryption.
Syntax	**disable password encryption**
Description	The user account configuration information will be stored in the configuration file, and can be applied to the system later. If the password encryption is enabled, the password will be in encrypted form when it is stored in the configuration file. When password encryption is disabled, if the user specifies the password in plain text form, the password will be in plan text form. However, if the user specifies the password in encrypted form, or if the password has been converted to encrypted form by the last enable password encryption command, the password will still be in the encrypted form. It can not be reverted to the plain text.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable password encryption:

```
DGS-3700-12:5#disable password encryption
Command: disable password encryption

Success.

DGS-3700-12:5#
```

show session

Purpose	Used to display a list of currently logged-in users.
Syntax	**show session**
Description	This command is used to display a list of all the users that are logged-in at the time the command is issued.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display a list of current logged-in users:

```
DGS-3700-12:5#show session
Command: show session

ID   Live Time       From           Level    Name
---  ---------       ------------   -----    -------
 8   00:00:16.250    Serial Port    5        Anonymous

Total Entries: 1

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

show switch

Purpose	Used to display general information about the Switch.
Syntax	**show switch**
Description	This command is used to display information about the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch's information:

```
DGS-3700-12:5#show switch
Command: show switch

Device Type        : DGS-3700-12 Gigabit Ethernet Switch
MAC Address        : 00-21-91-AF-37-D0
IP Address         : 10.24.73.21 (Manual)
VLAN Name          : default
Subnet Mask        : 255.0.0.0
Default Gateway    : 0.0.0.0
Boot PROM Version  : Build 1.00.B002
Firmware Version   : Build 1.00.B035
Hardware Version   : A1
System Name        :
System Location    :
System Contact     :
Spanning Tree      : Disabled
GVRP               : Disabled
IGMP Snooping      : Disabled
MLD Snooping       : Disabled
TELNET             : Enabled (TCP 23)
WEB                : Enabled (TCP 80)
SNMP               : Disabled
SSL Status         : Disabled
SSH Status         : Disabled
802.1x             : Disabled

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

show device_status

Purpose	Used to display the current Switch power, temperature and fan status.
Syntax	**show device_status**
Description	This command is used to display status of both the Switch's internal and external power, temperature, and fan status.
Parameters	None.
Restrictions	None.

Example usage:

To display the Switch status:

```
DGS-3700-12:5#show device_status
Command: show device_status

Power Status   Temperature (Celsius)    Side Fan Status
-------------  ----------------------  -------------------------
 AC Active        Sensor  1 : 255        Fan  1 OK   : 12775 RPM
 DC Fail                                 Fan  2 OK   : 12775 RPM
                                         Fan  3 OK   : 12775 RPM

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

show serial_port

Purpose	Used to display the current serial port settings.
Syntax	**show serial_port**
Description	This command is used to display the current serial port settings.
Parameters	None.
Restrictions	None.

Example usage:

To display the serial port settings:

```
DGS-3700-12:5#show serial_port
Command: show serial_port

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

DGS-3700-12:5#
```

config serial_port

Purpose	Used to configure the serial bit rate that will be used to communicate with the management host and the auto logout time for idle connections.
Syntax	**config serial_port {baud_rate [9600 | 19200 | 38400 | 115200] | auto_logout [never | 2_minutes | 5_minutes | 10_minutes | 15_minutes]}(1)**
Description	This command is used to configure the serial bit rate that will be used to communicate with the management host and the auto logout time for idle connections.
Parameters	*baud_rate [9600 | 19200 | 38400 | 115200]* – The serial bit rate that will be used to communicate with the management host. There are four options: 9600, 19200, 38400, 115200. Factory default setting is 115200. *never* – No time limit on the length of time the console can be open with no user input. *2_minutes* – The console will log out the current user if there is no user input for 2 minutes. *5_minutes* – The console will log out the current user if there is no user input for 5 minutes. *10_minutes* – The console will log out the current user if there is no user input for 10 minutes. *15_minutes* – The console will log out the current user if there is no user input for 15 minutes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure baud rate:

```
DGS-3700-12:5#config serial_port baud_rate 115200
Command: config serial_port baud_rate 115200

Success.

DGS-3700-12:5#
```

NOTE: If a user configures the serial port's baud rate, the baud rate will take effect and save immediately. Baud rate settings will not change even if the user resets or reboots the Switch. The Baud rate will only change when the user configures it again. The serial port's baud rate setting is not stored in the Switch's configuration file. Resetting the Switch will not restore the baud rate to the default setting.

enable clipaging

Purpose	Used to pause the scrolling of the console screen when a command displays more than one page.
Syntax	**enable clipaging**
Description	This command is used when issuing a command which causes the console screen to rapidly scroll through several pages. This command will cause the console to pause at the end of each page. The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3700-12:5#enable clipaging
Command: enable clipaging

Success.

DGS-3700-12:5#
```

disable clipaging

Purpose	Used to disable the pausing of the console screen scrolling at the end of each page when a command displays more than one screen of information.
Syntax	**disable clipaging**
Description	This command is used to disable the pausing of the console screen at the end of each page when a command would display more than one screen of information.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3700-12:5#disable clipaging
Command: disable clipaging

Success.

DGS-3700-12:5#
```

enable telnet

Purpose	Used to enable communication with and management of the Switch using the Telnet protocol.
Syntax	**enable telnet <tcp_port_number 1-65535>**
Description	This command is used to enable the Telnet protocol on the Switch. The user can specify the TCP or UDP port number the Switch will use 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" TCP port for the Telnet protocol is 23.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable Telnet and configure port number:

```
DGS-3700-12:5#enable telnet 23
Command: enable telnet 23

Success.

DGS-3700-12:5#
```

disable telnet

Purpose	Used to disable the Telnet protocol on the Switch.
Syntax	**disable telnet**
Description	This command is used to disable the Telnet protocol on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the Telnet protocol on the Switch:

```
DGS-3700-12:5#disable telnet
Command: disable telnet

Success.

DGS-3700-12:5#
```

enable web

Purpose	Used to enable the HTTP-based management software on the Switch.
Syntax	**enable web <tcp_port_number 1-65535>**
Description	This command is used to enable the Web-based management software on the Switch. The user can specify the TCP port number the Switch will use 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 and Operator-level users can issue this command.

Example usage:

To enable HTTP and configure port number:

```
DGS-3700-12:5#enable web 80
Command: enable web 80

Success.

DGS-3700-12:5#
```

disable web

Purpose	Used to disable the HTTP-based management software on the Switch.
Syntax	**disable web**
Description	This command disables the Web-based management software on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable HTTP:

```
DGS-3700-12:5#disable web
Command: disable web

Success.

DGS-3700-12:5#
```

save

Purpose	Used to save changes in the Switch's configuration to non-volatile RAM.
Syntax	**save {[config <config_id 1-2> | log | all]}**
Description	This command is 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* <*config_id 1-2*> – Specify to save current settings to configuration file 1 or 2. *log* – Specify to save current Switch log to NV-RAM. *all* – Specify to save all configuration settings. If nothing is specified after "save", the Switch will save all current configuration to non-volatile RAM.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3700-12:5#save
Command: save

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

DGS-3700-12:5#
```

reboot

Purpose	Used to restart the Switch.
Syntax	**Reboot {force_agree}**
Description	This command is used to restart the Switch.
Parameters	*force_agree* – When force_agree is specified, the reboot command will be executed immediatedly without further confirmation.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To restart the Switch:

```
DGS-3700-12:5#reboot
Command: reboot
Are you sure you want to proceed with the system reboot? (y|n)y
Please wait, the switch is rebooting...
```

reset

Purpose	Used to reset the Switch to the factory default settings.
Syntax	**reset {[config |system]} {force_agree}**
Description	This command is used to restore 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. *force_agree* – When force_agree is specified, the reset command will be executed immediatedly without further confirmation. If no parameter is specified, the Switch's current IP address, banner, 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.  **NOTE:** The serial port baud rate will not be changed by the reset command. It will not be restored to the factory default setting.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

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

```
DGS-3700-12:5#reset config
Command: reset config

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

Success.

DGS-3700-12:5#
```

login

Purpose	Used to log in a user to the Switch's console.
Syntax	**login**
Description	This command is used to initiate the login procedure. The user will be prompted for a Username and Password.
Parameters	None.
Restrictions	None.

Example usage:

To initiate the login procedure:

```
DGS-3700-12:5#login
Command: login

UserName:
```

logout

Purpose	Used to log out a user from the Switch's console.
Syntax	**logout**
Description	This command terminates the current user's session on the Switch's console.
Parameters	None.
Restrictions	None.

Example usage:

To terminate the current user's console session:

```
DGS-3700-12:5#logout
```

5

MODIFY BANNER AND PROMPT COMMANDS

Administrator level users can modify the login banner (greeting message) and command prompt by using the commands described below.

Command	Parameters
config command_ prompt	[<string 16> | username | default]
config greeting_message	{default}
show greeting_message	

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

config command prompt

Purpose	Used to configure the command prompt.
Syntax	**config command_prompt [<string 16> | username | default]**
Description	This command is for users to change the command prompt.
Parameters	*string 16* –The command prompt can be changed by entering a new name of no more that 16 characters. *username* – The command prompt will be changed to the login username. *default* – The command prompt will reset to factory default command prompt.
Restrictions	Only Administrator and Operator-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-3700-12:5#config command_prompt AtYourService
Command: config command_prompt AtYourService

Success.

AtYourService:admin5#
```

config greeting _message

Purpose	Used to configure the login banner (greeting message).
Syntax	**config greeting _message {default}**
Description	This command is used 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 settings: Ctrl+X Reload original settings: Ctrl+L
Restrictions	Only Administrator and Operator-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**" command to save it into FLASH. • Only valid in threshold level.

Example usage:

To modify the banner:

```
DGS-3700-12:5#config greeting_message
Command: config greeting_message

Greeting Messages Editor
================================================================================
                        DGS-3700-12G Gigabit Ethernet Switch
                           Command Line Interface

                         Firmware: Build 1.00.B042
           Copyright(C) 2009 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	This 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-3700-12:5#show greeting_message
Command: show greeting_message

      ================================================================================
                        DGS-3700-12G Gigabit Ethernet Switch
                              Command Line Interface

                             Firmware: Build 1.00.B042
                  Copyright(C) 2009 D-Link Corporation. All rights reserved.
      ================================================================================

DGS-3700-12:5#
```

6

SWITCH UTILITY COMMANDS

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

Command	Parameters
download	[firmware_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {image_id <int 1-2>} | cfg_fromTFTP [<ipaddr> | <ipv6addr>] <path_filename 64> {[<config_id 1-2> | increment]}]
config firmware	image_id <int 1-2> [delete | boot_up]
show firmware information	
show config	[current_config | config_in_nvram <config_id 1-2> | information]
upload	[cfg_toTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> { <config_id 1-2>}| log_toTFTP [<ipaddr> |<ipv6addr>] path_filename 64> | attack_log_toTFTP [<ipaddr> |<ipv6addr>] <path_filename 64>]
enable autoconfig	
disable autoconfig	
show autoconfig	
config configuration	<config_id 1-2> [boot_up | delete | active]
ping	<ipaddr> {times <value 1-255>} {timeout <sec 1-99>}
ping6	<ipv6addr> {times <value 1-255>| size <value 1-6000>| timeout <value 1-10>}

Each command is listed, in detail, in the following sections.

download

Purpose	Used to download and install new firmware or a Switch configuration file from a TFTP server.
Syntax	**download [firmware_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {image_id <int 1-2>} | cfg_fromTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> {[<config_id 1-2> | increment]}]**
Description	This command is used to download a new firmware or a Switch configuration file from a TFTP server.
Parameters	*firmware_fromTFTP* – Download and install new firmware on the Switch from a TFTP server. *cfg_fromTFTP* – Download a switch configuration file from a TFTP server. *<ipaddr>* – The IP address of the TFTP server. *<ipv6addr>* – The IPv6 address of the TFTP server. *<path_filename>* – The DOS path and filename of the firmware or switch configuration file on the TFTP server. For example, C:\3700.had. *image_id <int 1-2>* – Specify the working section ID. The Switch can hold two firmware versions for the user to select from, which are specified by section ID. *config_id <1-2>* - Specifes the configuration identify number of the indicated configuration. *increment* – Allows the download of a partial switch configuration file. This allows a file to be downloaded that will change only the switch parameters explicitly stated in the configuration file. All other switch parameters will remain unchanged.
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only Administrator-level users can issue this command.

Example usage:

To download a configuration file:

```
DGS-3700-12:5#download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt
Command: download cfg_fromTFTP 10.48.74.121 c:\cfg\setting.txt

Connecting to server.................. Done.
Download configuration................. Done.

DGS-3700-12:5#
DGS-3700-12:5##-------------------------------------------------------------
DGS-3700-12:5##                DGS-3700-12 Configuration
DGS-3700-12:5##
DGS-3700-12:5##               Firmware: Build 1.00.B042
DGS-3700-12:5##Copyright(C) 2009 D-Link Corporation. All rights reserved.
DGS-3700-12:5##-------------------------------------------------------------
DGS-3700-12:5#
DGS-3700-12:5#
DGS-3700-12:5## BASIC
DGS-3700-12:5#
DGS-3700-12:5#config serial_port baud_rate 115200 auto_logout 10_minutes
Command: config serial_port baud_rate 115200 auto_logout 10_minutes
```

The download configuration command will initiate the loading of the various settings in the order listed in the configuration file. When the file has been successfully loaded the message "End of configuration file for DGS-3700-12" appears followed by the command prompt.

```
DGS-3700-12:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-3700-12:5#
DGS-3700-12:5##-------------------------------------------------------
DGS-3700-12:5##        End of configuration file for DGS-3700-12
DGS-3700-12:5##-------------------------------------------------------
DGS-3700-12:5#
```

config firmware

Purpose	Used to configure the firmware section as a boot up section, or to delete the firmware section
Syntax	**config firmware image_id <int 1-2> [delete | boot_up]**
Description	This command is used to configure the firmware section. The user may choose to remove the firmware section or use it as a boot up section.
Parameters	*image_id* – Specifies the working section. The Switch can hold two firmware versions for the user to select from, which are specified by image ID. *delete* – Entering this parameter will delete the specified firmware section. *boot_up* – Entering this parameter will specify the firmware image ID as a boot up section.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure firmware image 1 as a boot up section:

```
DGS-3700-12:5#config firmware image_id 1 boot_up
Command: config firmware image_id 1 boot_up

Success.

DGS-3700-12:5#
```

show firmware information

Purpose	Used to display the firmware section information.
Syntax	**show firmware information**
Description	This command is used to display the firmware section information.
Parameters	None.
Restrictions	None.

Example usage:

To display the current firmware information on the Switch:

```
DGS-3700-12:5#show firmware information
Command: show firmware information

 Image ID    : 1(Boot up firmware)
 Version     : 1.00.B035
 Size        : 2562816 Bytes
 Update Time: 2000/01/01 00:13:55
 From        : 10.73.21.1(Console)
 User        : Anonymous

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

DGS-3700-12:5#
```

show config

Purpose	Used to display the current or saved version of the configuration settings of the switch.
Syntax	**show config [current_config | config_in_nvram <config_id 1-2> | information]**
Description	This command is used to display all the configuration settings that are saved to NV RAM or display the configuration settings as they are currently configured. Use the keyboard to list settings one line at a time (Enter), one page at a time (Space) or view all (a). The configuration settings are listed by category in the following order: 1. Basic (serial port, Telnet and web management status) 2. storm control 3. IP group management 4. syslog 5. QoS 6. port mirroring 7. traffic segmentation 8. port 9. port lock 10. 8021x 11. SNMPv3 12. management (SNMP traps RMON) 13. VLAN 14. FDB (forwarding data base) 15. MAC address table notification 16. STP 17. SSH 18. SSL 19. ACL 20. SNTP 21. IP route 22. LACP 23. ARP 24. IP 25. IGMP snooping 26. access authentication control (TACACS etc.)
Parameters	*current_config* – Entering this parameter will display configurations entered without being saved to NVRAM. *config_in_NVRAM* – Entering this parameter will display configurations entered and saved to NVRAM. *information* – Entering this parameter will display the global information for the configuration settings.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view the current configuration settings:

```
DGS-3700-12:5#show config current_config
Command: show config current_config

#------------------------------------------------------
#                  DGS-3700-12 Configuration
#
#                Firmware: Build 1.00.B042
# Copyright(C) 2009 D-Link Corporation. All rights reserved.
#------------------------------------------------------


# STACK



# BASIC

# ACCOUNT LIST
# ACCOUNT END
# PASSWORD ENCRYPTION
disable password encryption
config serial_port auto_logout 10_minutes
enable telnet 23
enable web 80

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

upload

Purpose	Used to upload the current switch settings or the switch history log to a TFTP.
Syntax	**[cfg_toTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> { <config_id 1-2>}| log_toTFTP [<ipaddr> |<ipv6addr>] <path_filename 64> | attack_log_toTFTP [<ipaddr> |<ipv6addr>] <path_filename 64>]**
Description	This command is used to upload either the Switch's current settings or the Switch's history log to a TFTP server.
Parameters	*cfg_toTFTP* – Specifies that the Switch's current settings will be uploaded to the TFTP server. *log_toTFTP* – Specifies that the switch history log will be uploaded to the TFTP server. *attack_log_toTFTP* – Specifies that the switch attack log will be uploaded to the TFTP server. <*ipaddr*> – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the Switch. <*ipv6addr*> – The IPv6 address of the TFTP server. <*path_filename 64*> – Specifies the location of the Switch configuration file on the TFTP server. This file will be replaced by the uploaded file from the Switch.
Restrictions	The TFTP server must be on the same IP subnet as the Switch. Only Administrator and Operator-level users can issue this command.

Example usage:

To upload a configuration file:

```
DGS-3700-12:5#upload cfg_toTFTP 10.48.74.121 c:\cfg\configuration.txt
Command: upload cfg_toTFTP 10.48.74.121 c:\cfg\configuration.txt

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

DGS-3700-12:5#
```

enable autoconfig

Purpose	Used to activate the autoconfiguration 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 autoconfiguration process the previously saved local configuration file present in Switch memory will be loaded. Only Administrator and Operator-level users can issue this command.

NOTE: Dual-purpose (DHCP/TFTP) server utility software may require entry of the configuration file name and path within the user interface. Alternatively, the DHCP software may require creating a separate ext file with the configuration file name and path in a specific directory on the server. Consult the documentation for the DCHP server software if users are unsure.

Example usage:

To enable autoconfiguration on the Switch:

```
DGS-3700-12:5#enable autoconfig
Command: enable autoconfig

Success.

DGS-3700-12:5#
```

When autoconfig is enabled and the Switch is rebooted, the normal login screen will appear for a few moments while the autoconfig request (i.e. download configuration) is initiated. The console will then display the configuration parameters as they are loaded from the configuration file specified in the DHCP or TFTP server. This is exactly the same as using a **download configuration** command. After the entire Switch configuration is loaded, the Switch will automatically "logout" the server. The configuration settings will be saved automatically and become the active configuration.

Upon booting up the autoconfig process is initiated, the console screen will appear similar to the example below. The configuration settings will be loaded in normal order.

```
      DGS-3700-12 Fast Ethernet Switch Command Line Interface

                  Firmware: Build 1.00.B042
    Copyright(C) 2009 D-Link Corporation. All rights reserved.

DGS-3700-12:5#
DGS-3700-12:5#
DGS-3700-12:5#download configuration 10.41.44.44 c:\cfg\setting.txt
Command: download configuration 10.41.44.44 c:\cfg\setting.txt

Connecting to server.................. Done.
Download configuration................. Done.
```

The very end of the autoconfig process including the logout appears like this:

```
DGS-3700-12:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-3700-12:5#
DGS-3700-12:5##-------------------------------------------------------------
DGS-3700-12:5##          End of configuration file for DGS-3700-12
DGS-3700-12:5#

**********
* Logout *
**********
```

NOTE: With autoconfig enabled, the Switch ipif settings now define the Switch as a DHCP client. Use the **show switch** command to display the new IP settings status.

disable autoconfig

Purpose	Use this to deactivate autoconfiguration from DHCP.
Syntax	**disable autoconfig**
Description	This command is used to instruct the Switch not to accept autoconfiguration 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 and Operator-level users can issue this command.

Example usage:

To stop the autoconfiguration function:

```
DGS-3700-12:5#disable autoconfig
Command: disable autoconfig

Success.

DGS-3700-12:5#
```

show autoconfig

Purpose	Used to display the current autoconfig status of the Switch.
Syntax	**show autoconfig**
Description	This command will list the current status of the autoconfiguration function.
Parameters	None.
Restrictions	None.

Example usage:

To display autoconfig:

```
DGS-3700-12:5#show autoconfig
Command: show autoconfig
Autoconfig State: Disabled.

Success.

DGS-3700-12:5#
```

config configuration

Purpose	Used to configure specific firmware as a boot up image.
Syntax	**config configuration <config_id 1-2> [boot_up | delete| active]**
Description	This command is used to configure a specific boot up image.
Parameters	*<config_id 1-2>* – Specifies the serial number of the indicated configuration. *boot_up* – Specifies the config is boot_up config. *delete* – Delete the configuration. *active* – Active specifies the configuration .
Restrictions	You must have Administrator-level privileges.

Example usage:

To configure the specific configuration as boot up image:

```
DGS-3700-12:5#config configuration 2 boot_up
Command: config configuration 2 boot_up

Success.
DGS-3700-12:5#
```

ping

Purpose	Used to test the connectivity between network devices.
Syntax	**ping <ipaddr> {times <value 1-255>} {timeout <sec 1-99>}**
Description	This command is used to send Internet Control Message Protocol (ICMP) echo messages to a remote IP address. The remote IP address will then "echo" or return the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	*<ipaddr>* - Specifies the IP address of the host. *times <value 1-255>* - The number of individual ICMP echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. *timeout <sec 1-99>* - Defines the time-out period while waiting for a response from the remote device. A value of 1 to 99 seconds can be specified. The default is 1 second.
Restrictions	None.

Example usage:

To ping the IP address 10.48.74.121 four times:

```
DGS-3700-12:5#ping 10.48.74.121 times 4
Command: ping 10.48.74.121

Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms
Reply from 10.48.74.121, time<10ms

Ping statistics for 10.48.74.121
Packets: Sent =4, Received =4, Lost =0

DGS-3700-12:5#
```

ping6

Purpose	Used to test the connectivity between network devices.
Syntax	**ping6 <ipv6addr> {times <value 1-255>| size <value 1-6000>| timeout<value 1-10>}**
Description	This command is used to send Internet Control Message Protocol (ICMPv6) echo messages to a remote IP address. The remote IPv6 address will then "echo" or return the message. This is used to confirm connectivity between the Switch and the remote device.
Parameters	< *ipv6addr* > – Specifies the IPv6 address of the host. *times <value 1-255>* – The number of individual ICMPv6 echo messages to be sent. A value of 0 will send an infinite ICMP echo messages. The maximum value is 255. The default is 0. *size <value 1-6000>* – Use this parameter to set the datagram size of the packet, or in essence, the number of bytes in each ping packet. Users may set a size between 1 and 6000 bytes with a default setting of 100 bytes. *timeout <value 1-10>* – Select a timeout period between 1 and 10 seconds for this Ping message to reach its destination. If the packet fails to find the IPv6 address in this specified time, the Ping packet will be dropped.
Restrictions	None.

Example usage:

To ping the IPv6 address 1001::3702 four times:

```
DGS-3700-12:5#ping6 1001::3702 times 4
Command: ping6 1001::3702 times 4

Reply from 1001::3702, bytes=100 time<10 ms
Reply from 1001::3702, bytes=100 time<10 ms
Reply from 1001::3702, bytes=100 time<10 ms
Reply from 1001::3702, bytes=100 time<10 ms
 Ping Statistics for 1001::3702
 Packets: Sent =4, Received =4, Lost =0

DGS-3700-12:5#
```

7

BASIC IP COMMANDS

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

Command	Parameters
config ipif	<ipif_name 12> [{ipaddress <network_address> |vlan <vlan_name 32> |state [enable |disable]} (1) | bootp |dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable| disable]] |ipv4 state [enable | disable]]
create ipif	<ipif_name 12> {<network_address>} <vlan_name 32> {state [enable|disable]}
delete ipif	[<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]
show ipif	{<ipif_name 12>}
enable ipif	[<ipif_name 12> | all]
disable ipif	[<ipif_name 12> | all]
enable autoconfig*	
disable autoconfig	
show autoconfig	
enable ipif_ipv6_link_local_auto	[<ipif_name 12> | all]
disable ipif_ipv6_link_local_auto	[<ipif_name 12> | all]
show ipif_ipv6_link_local_auto	{<ipif_name 12>}

Each command is listed, in detail, in the following sections.

*See Switch Utility Commands for descriptions of all autoconfig commands.

config ipif

Purpose	Used to configure the IP interface.
Syntax	**config ipif <ipif_name 12> [{ipaddress <network_address> |vlan <vlan_name 32> |state [enable |disable]}(1) | bootp |dhcp | ipv6 [ipv6address <ipv6networkaddr> | state [enable| disable]] |ipv4 state [enable | disable]]**
Description	This command is used to configure the IP interface on the Switch.
Parameters	*<ipif_name 12>* – Enter an alphanumeric string of up to 12 characters to identify this IP interface. *ipaddress <network_address>* – IP address and netmask of the IP interface to be created. Users can specify the address and mask information using the traditional format (for example, 10.1.2.3/255.0.0.0) or in CIDR format (10.1.2.3/8). *<vlan_name 32>* – The name of the VLAN corresponding to the System IP interface. *state [enable | disable]* – Allows users to enable or disable the IP interface. *bootp* – Allows the selection of the BOOTP protocol for the assignment of an IP address to the Switch's System IP interface. *dhcp* – Allows the selection of the DHCP protocol for the assignment of an IP address to the Switch's System IP interface. If users are using the autoconfig feature, the Switch becomes a DHCP client automatically so it is not necessary to change the ipif settings. *ipv6address* – 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 ipif. *Ipv6 state* – Allows users to enable IPv6 address on the IP interface. *ipv4 state* – Allows users to enable IPv4 address on the IP interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the IP interface System:

```
DGS-3700-12:5#config ipif System ipaddress 10.48.74.122/8
Command: config ipif System ipaddress 10.48.74.122/8

Success.

DGS-3700-12:5#
```

create ipif

Purpose	Used to create a L3 interface.
Syntax	**create ipif <ipif_name 12> {<network_address>} <vlan_name 32> {state [enable|disable]}**
Description	This command creates a L3 interface. This interface can be configured with IPv4 or IPv6 address. Currently, it has a restriction. An interface can have only one IPv4 address defined. But it can have multiple IPv6 addresses defined. Thus, the multinetting configuration of IPv4 must be done through the creation of a secondary interface on the same VLAN, instead of directly configuring multiple IPv4 addresses on the same interface. Configuration of IPv6 addresses must be done through the command config ipif.
Parameters	*<ipif_name 12>* – The name created for the IP interface. <network_address> – The network address for the IP interface to be created. *<vlan_name 32>* – The name of vlan *state – the state of interface .*
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an interface

```
DGS-3700-12:5#create ipif if2 vlan2 state enable
Command: create ipif if2 vlan2 state enable

Success.

DGS-3700-12:5#
```

delete ipif

Purpose	This command is used to delete an interface.
Syntax	**delete ipif [<ipif_name 12> {ipv6address <ipv6networkaddr>} | all]**
Description	This command is used to delete an interface, all interfaces, or the ipv6 address of the interface. Note that the system interface can not be deleted. By using this command, an IPv6 address can be deleted from the ipif.
Parameters	*<ipif_name 12>* – The name of the deleted IP interface. *ipv6address <ipv6networkaddr>* – The IPv6 address which will be deleted from the interface.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP interface.

```
DGS-3700-12:5#delete ipif  if2
Command: delete ipif if2

Success.

DGS-3700-12:5#
```

To delete an IPV6 address from the interface :

```
DGS-3700-12:5#delete ipif if2 ipv6address 5001::3700/8
Command: delete ipif if2 ipv6address 5001::3700/8

Success.

DGS-3700-12:5#
```

enable ipif

Purpose	Used to enable the admin state for an interface.
Syntax	**enable ipif [<ipif_name 12> | all]**
Description	This command is used to enable the state for an IPIF. When the state is enabled, the IPv4 processing will be started. When the IPv4 address is configured on the IPIF. The IPv6 processing will be started when the IPv6 address is explicitly configured on the IPIF.
Parameters	*<ipif_name 12>* – The name of the IP interface. *all* – All the interface
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the admin state of one interface .

```
DGS-3700-12G:5#enable ipif System
Command: enable ipif System

Success.

DGS-3700-12G:5#
```

disable ipif

Purpose	Used to disable the admin state for an interface.
Syntax	**disable ipif [<ipif_name 12> | all]**
Description	This command is used to disable the state for an ipif.
Parameters	*<ipif_name 12>* – The name of the IP interface. *all* – Specifies all interfaces.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the admin state for an interface.

```
DGS-3700-12G:5#disable ipif System
Command: disable ipif System

Success.

DGS-3700-12G:5#
```

show ipif

Purpose	Used to display the configuration of an IP interface on the Switch.
Syntax	**show ipif {<ipif_name 12>}**
Description	This command is used to display the configuration of an IP interface on the Switch.
Parameters	*<ipif_name 12>* – The name created for the IP interface.
Restrictions	None.

Example usage:

To display IP interface settings.

```
DGS-3700-12:5#show ipif System
Command: show ipif System

IP Interface                : System
VLAN Name                   : default
Interface Admin State       : Enabled
Link Status                 : LinkUp
IPv4 Address                : 10.24.73.21/8 (Manual)  Primary
IPv4 State                  : Enabled

DGS-3700-12:5#
```

enable autoconfig

Purpose	Used to activate the autoconfiguration 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 boot file or configuration file. Only Administrator and Operator-level users can issue this command.

Example usage:

To enable autoconfiguration on the Switch:

```
DGS-3700-12:5#enable autoconfig
Command: enable autoconfig

Success.

DGS-3700-12:5#
```

NOTE: More detailed information for this command and related commands can be found in the section titled Switch Utility Commands.

disable autoconfig

Purpose	Used to disable the auto configuration function.
Syntax	**disable autoconfig**
Description	When auto configuration is disabled, the switch will configure itself using the local configuration file.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the auto configuration function:

```
DGS-3700-12:5#disable autoconfig
Command:disable autoconfig

Success.

DGS-3700-12:5#
```

show autoconfig

Purpose	Used to display the auto configuration status.
Syntax	**show autoconfig**
Description	The command is used to show autoconfig enable or disable status.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the auto configuration status:

```
DGS-3700-12:5#show autoconfig
Command: show autoconfig

Autoconfig State: Disabled

DGS-3700-12:5#
```

enable ipif_ipv6_link_local_auto

Purpose	This command enables the auto configuration of link local addresses when no IPv6 address is configured.
Syntax	**enable ipif_ipv6_link_local_auto [<ipif_name 12> | all]**
Description	This command is used to enable the auto configuration of link local addresses when there are no IPv6 addresses explicitly configured. When an IPv6 address is explicitly configured, the link local address will be automatically configured, and the IPv6 processing will be started. When there is no IPv6 address explicitly configured, by default, link local address is not configured and the IPv6 processing will be disabled. By enabling this automatic configuration, the link local address will be automatically configured and IPv6 processing will be started.
Parameters	*<ipif_name 12>* – The name of the IP interface. *all* – Indidcates all IP interfaces.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the automatic configuration of link local address for an interface:

```
DGS-3700-12:5#enable ipif_ipv6_link_local_auto all
Command: enable ipif_ipv6_link_local_auto all

Success.

DGS-3700-12:5#
```

disable ipif_ipv6_link_local_auto

Purpose	Disables the auto configuration of link local addresses when no IPv6 addresses are configured.
Syntax	**disable ipif_ipv6_link_local_auto [<ipif_name 12> | all]**
Description	This command is used to disable the auto configuration of link local addresses when no IPv6 address is explicitly configured.
Parameters	*<ipif_name 12>* – The name of the IP interface. *all* – Indicates all IP interfaces.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the automatic configuration of link local address for an interface:

```
DGS-3700-12:5#disable ipif_ipv6_link_local_auto System
Command: disable ipif_ipv6_link_local_auto System

Success.

DGS-3700-12:5#
```

show ipif_ipv6_link_local_auto

Purpose	Displays the link local address automatic configuration state.
Syntax	**show ipif_ipv6_link_local_auto {<ipif_name 12>}**
Description	This command is used to display the link local address automatic configuration state.
Parameters	*<ipif_name 12>* – The name created for the IP interface.
Restrictions	None.

Example usage:

To display the link local address automatic configuration state:

```
DGS-3700-12:5#show ipif_ipv6_link_local_auto
Command: show ipif_ipv6_link_local_auto

 IPIF: System          Automatic Link Local Address: Disabled

DGS-3700-12:5#
```

8

ROUTING TABLE COMMANDS

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

Command	Parameters
create iproute	[default] <ipaddr> {<metric 1-65535>}{[primary|backup]}
delete iproute	[default] <ipaddr>
show iproute	{static}
create ipv6route	[default] [<ipif_name 12> <ipv6addr>| <ipv6addr>] {<metric 1-65535>} {primary | backup}
delete ipv6route	[default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]
show ipv6route	

Each command is listed, in detail, in the following sections.

create iproute default

Purpose	Used to create IP route entries to the Switch's IP routing table.
Syntax	**create iproute [default] <ipaddr> {<metric 1-65535>}{[primary|backup]}**
Description	This command is used to create a default static IP route entry to the Switch's IP routing table.
Parameters	*<ipaddr>* – The gateway IP address for the next hop router. *<metric 1-65535>* – Allows the entry of a routing protocol metric entry representing the number of routers between the Switch and the IP address above. The default setting is 1.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add the default static address 10.48.74.121, with a metric setting of 1, to the routing table:

```
DGS-3700-12:5#create iproute default 10.48.74.121 1
Command: create iproute default 10.48.74.121 1

Success.

DGS-3700-12:5#
```

delete iproute default

Purpose	Used to delete a default IP route entry from the Switch's IP routing table.
Syntax	**delete iproute [default]**
Description	This command will delete an existing default entry from the Switch's IP routing table.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the default IP route 10.53.13.254:

```
DGS-3700-12:5#delete iproute default
Command: delete iproute default

Success.

DGS-3700-12:5#
```

show iproute

Purpose	Used to display the Switch's current IP routing table.
Syntax	**show iproute**
Description	This command will display the Switch's current IP routing table.
Parameters	None.
Restrictions	None.

Example usage:

To display the contents of the IP routing table:

```
DGS-3700-12:5#show iproute
Command: show iproute

Routing Table

IP Address/Netmask  Gateway     Interface    Cost    Protocol
---------------     ---------   ------------ ----   -----------
0.0.0.0             10.1.1.254   System       1      Default
10.0.0.0/8          10.48.74.122 System       1      Local

Total Entries: 2

DGS-3700-12:5#
```

create ipv6route default

Purpose	create an ipv6 default gateway.
Syntax	**create ipv6route [default] [<ipif_name 12> <ipv6addr>| <ipv6addr>] {<metric 1-65535>} {primary | backup}**
Description	This command is used to create a primary and backup IPv6 default gateway.
Parameters	*default* – Use this parameter to create an IPv6 default gateway. *<ipif_name 12>* – Enter the corresponding ipif name of the IPv6 address. *<ipv6addr>* − IPv6 address for the next hop router. *<metric 1-65535>* − Allows the entry of a routing protocol metric entry, representing the number of routers between the Switch and the IP address above. The default setting is 1. *[primary | backup]* – The user may choose between Primary and Backup. If the Primary Static/Default Route fails, the Backup Route will support the entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Create an ipv6 default gateway:

```
DGS-3700-12:5#create ipv6route default System 3FFE::1 33 primary
Command: create ipv6route default System 3FFE::1 33 primary
Success.

DGS-3700-12:5#
```

delete ipv6route

Purpose	delete an ipv6 default gateway.
Syntax	**delete ipv6route [default] [<ipif_name 12> <ipv6addr> | <ipv6addr> | all]**
Description	This command is used to delete an ipv6 route.
Parameters	*default* – Use this parameter to delete an IPv6 default gateway. *<ipif_name 12>* – Enter the corresponding ipif name of the IPv6 address. *<ipv6addr>* − IPv6 address for the next hop router. *all* − This will delete all IPv6 default gateways.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

Delete an ipv6 default route:

```
DGS-3700-12:5#delete ipv6route default  System 3ffe::1
Command: delete ipv6route default  System 3ffe::1

Success.
DGS-3700-12:5#
```

show ipv6route

Purpose	Used to display the Switch's current IPv6 route.
Syntax	**show ipv6route**
Description	This command will display the Switch's current IPv6 route.
Parameters	None.
Restrictions	None.

Example usage:

To display the static IPv6 entries in the routing table:

```
DGS-3700-12:5#show ipv6route
Command: show ipv6route

IPv6 Prefix: 3001:: /64                Protocol : Static         Metric: 1
Next Hop   : 3101::1                   IPIF     : System
Backup     : primary                   Status   : active

Total Entries: 1

DGS-3700-12:5#
```

9

IPV6 NEIGHBOR DISCOVERY COMMANDS

The following commands are used to detect IPv6 neighbors on the switch and to keep a running database about these neighbor devices. The IPv6 Neighbor Detection commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create ipv6 neighbor_cache ipif	<ipif_name 12> <ipv6addr> <macaddr>
delete ipv6 neighbor_cache ipif	[<ipif_name 12> | all][<ipv6addr> |static |dynamic | all]
show ipv6 neighbor_cache ipif	[<ipif_name 12> | all] [ipv6address <ipv6addr> | static | dynamic |all]
config ipv6 nd ns ipif	<ipif_name 12> retrans_time <uint 0-4294967295>
show ipv6 nd	{ipif <ipif_name 12>}

Each command is listed, in detail, in the following sections.

create ipv6 neighbor_cache ipif

Purpose	This command is used to add a static IPv6 neighbor.
Syntax	**create ipv6 neighbor_cache ipif <ipif_name 12> <ipv6addr> <macaddr>**
Description	This command is used to add a static IPv6 neighbor to an existing IPv6 interface previously created on the switch.
Parameters	*<ipif_name 12>* – Enter the IPv6 interface name previously created using the create ipif command. *<ipv6addr>* – Enter the IPv6 address of the neighbor device to be added as an IPv6 neighbor of the IP interface previously entered in this command. *<macaddr>* – Enter the MAC address of the neighbor device to be added as an IPv6 neighbor of the IP interface previously entered in this command.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a static IPv6 neighbor:

```
DGS-3700-12:5#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-3700-12:5#
```

delete ipv6 neighbor_cache ipif

Purpose	Used to remove a static IPv6 neighbor.
Syntax	**delete ipv6 neighbor_cache ipif [<ipif_name 12> | all] [<ipv6addr> | static | dynamic | all]**
Description	This command is used to remove a static IPv6 neighbor from an existing IPv6 interface previously created on the switch.
Parameters	*<ipif_name 12>* – Enter the IPv6 interface name previously created using the **create ipif** commands. *all* – Enter this parameter to denote all IPv6 interfaces created on the switch. *<ipv6addr>* – Enter the IPv6 address of the neighbor device to be removed from being an IPv6 neighbor of the IP interface previously entered in this command. *static* – Enter this command to remove all statically configured neighbor devices from being an IPv6 neighbor of the IP interface previously entered. *dynamic* – Enter this command to remove all dynamically configured neighbor devices from being an IPv6 neighbor of the IP interface previously entered. *all* – Enter this parameter to remove all IPv6 neighbors of the switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a static IPv6 neighbor:

```
DGS-3700-12:5#delete ipv6 neighbor_cache ipif  System 3FFC::1
Command: delete ipv6 neighbor_cache ipif  System 3FFC::1
Success.

DGS-3700-12:5#
```

show ipv6 neighbor_cache ipif

Purpose	Used to view the neighbor cache of an IPv6 interface located on the Switch.
Syntax	**show ipv6 neighbor_cache ipif [<ipif_name 12> | all] | [ipv6address <ipv6addr> | static | dynamic | all]**
Description	This command is used to display the IPv6 neighbors of a configured IPv6 interface currently set on the switch. Users may specify an IP interface, IPv6 address or statically entered IPv6 addresses by which to view the neighbor cache.
Parameters	*<ipif_name 12>* – Enter the IP interface for which to view IPv6 neighbors. This will display all IPv6 neighbors of this interface. *all* – Enter this parameter to denote all IPv6 interfaces created on the switch. *ipv6address <ipv6addr>* – Enter the IPv6 address of the neighbor by which to view this information. *static* – Enter this parameter to view all statically entered IPv6 neighbors of the switch. *dynamic* – Enter this command to view all dynamically configured neighbor devices which are IPv6 neighbors of the IP interface previously entered. *all* – Enter this parameter to view all configured neighbor devices which are IPv6 neighbors of the IP interface previously entered.
Restrictions	None.

Example usage:

```
DGS-3700-12:5#show ipv6 neighbor_cache ipif System all
Command: show ipv6 neighbor_cache ipif System all

Neighbor                          Link Layer Address Interface    State
------------------------------  ----------------- ------------ -----
FE80::216:36FF:FEB5:48DF          00-16-36-B5-48-DF  System       S
FE80::230:65FF:FE98:BFAC          00-30-65-98-BF-AC  System       S
FE80::280:C8FF:FE25:9050          00-80-C8-25-90-50  System       S
FE80::2D0:BAFF:FEF4:3282          00-D0-BA-F4-32-82  System       S

Total Entries: 4

State:
(I) means Incomplete state. (R) means Reachable state.
(S) means Stale state.      (D) means Delay state.
(P) means Probe state.      (T) means Static state.


DGS-3700-12:5#
```

To display the IPv6 neighbors of a configured IP interface:

config ipv6 nd ns ipif

Purpose	Used to configure the parameters for Neighbor solicitation messages to be sent from the switch.
Syntax	**config ipv6 nd ns ipif <ipif_name 12> retrans_time <uint 0-4294967295>**
Description	This command will configure the parameters for Neighbor Solicitation messages sent from the switch. These messages are used to detect IPv6 neighbors on the switch.
Parameters	*<ipif_name 12>* – Enter the IPv6 interface name for which to dispatch Neighbor solicitation messages. *retrans_time <uint 0-4294967295>* – Use this field to set the interval, in milliseconds that the Switch will produce Neighbor Solicitation packets to be sent out over the local network. This is used to discover IPv6 neighbors on the local link. The user may select a time between 0 and 4294967295 milliseconds. Very fast intervals, represented by a low number, are not recommended for this field.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the retrans time of a configured IP interface:

```
DGS-3700-12:5#config ipv6 nd ns ipif System retrans_time 1000000
Command: config ipv6 nd ns ipif System retrans_time 1000000

Success.

DGS-3700-12:5#
```

show ipv6 nd

Purpose	Used to display information regarding Neighbor Detection on the switch.
Syntax	**show ipv6 nd {ipif <ipif_name 12>}**
Description	This command is used to show information regarding the IPv6 Neighbor Detection function of the switch. Users may specify an IP interface for which to view this information.
Parameters	*<ipif_name 12>* – Enter the IP interface of the IPv6 interface for which to view this information. Omitting this parameter will display all information regarding neighbor detection currently set on the switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the neighbor detection parameters for IPv6:

```
DGS-3700-12:5#show ipv6 nd
Command: show ipv6 nd


Interface Name            : System
NS Retransmit Time        : 1000000 (ms)

DGS-3700-12:5#
```

10

LIMITED IP MULTICAST ADDRESS

The Limited IP Multicast command allows the administrator to permit or deny access to a port or range of ports by specifying a range of multicast addresses. The Limited IP Multicast Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create mcast_filter_profile profile_id	[ipv4|ipv6] profile_id <value 1-60> profile_name <name 1-32>
config mcast_filter_profile	[profile_id < value 1-60>| profile_name <name 1-32>] { profile_name <name 1-32> | [add | delete] <mcast_address_list>}(1)
config mcast_filter_profile ipv6	[profile_id < value 1-60>| profile_name <name 1-32>] { profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)
delete mcast_filter_profile profile_id	[ipv4|ipv6] [<value 1-60> | all]
delete mcast_filter_profile profile_name	[ipv4|ipv6] <name 1-32>
show mcast_filter_profile	[ipv4|ipv6] { profile_id <value 1-60> | profile name < name 1-32 >}
config limited_multicast_addr ports	[ports <portlist> | vlanid <vlanid_list >] {[ipv4|ipv6]} {[add | delete] [profile_id <value 1-60> | profile_name <name 1-32>] | access [permit | deny]}(1)
show limited_multicast_addr ports	[ipv4|ipv6] [ports {<portlist>} | vlanid <vlanid_list >]
config max_mcast_group ports	[ipv4|ipv6] [ports <portlist> | vlanid <vlanid_list] max_group [<value 1-1024> | infinite]}(1)
show max_mcast_group ports	[ipv4|ipv6] [ports <portlist>} | vlanid <vlanid_list >]

Each command is listed, in detail, in the following sections.

create mcast_filter_profile profile_id

Purpose	This command creates a multicast address profile.
Syntax	**create mcast_filter_profile [ipv4|ipv6] profile_id <value 1-60> <name 1-32>**
Description	This command configures a multicast address profile. Mutliple ranges of multicast addresses can be defined in the profile.
Parameters	*profile_id* – ID of the profile. The range is *1* to *60*. *<name 1-32>* – Provides a meaningful description for the profile.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a multicast filter profile:

```
DGS-3700-12:5#create mcast_filter_profile ipv4 profile_id 2 profile_name RG
Command: create mcast_filter_profile ipv4 profile_id 2 profile_name RG

Success.

DGS-3700-12:5#
```

config mcast_filter_profile

Purpose	This command adds or deletes a range of multicast addresses to the profile.
Syntax	**config mcast_filter_profile [profile_id < value 1-60>| profile_name <name 1-32>] { profile_name <name 1-32> | [add | delete] <mcast_address_list>}(1)**
Description	This command allows the user to add or delete a range of multicast IP addresses previously defined.
Parameters	*profile_id* – ID of the profile. The range is *1* to *60*. *profile_name* – Provides a meaningful description for the profile. *mcast_address_list* – List of the multicast addresses to be put in the profile. You can either specifiy a single multicast IP address or a range of multicast addresses using.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config an IPv4 multicast filter profile:

```
DGS-3700-12:5#config mcast_filter_profile profile_id 2 add 225.1.1.1-225.1.1.1
Command: config mcast_filter_profile profile_id 2 add 225.1.1.1

Success.

DGS-3700-12:5#
```

config mcast_filter_profile ipv6

Purpose	This command adds or deletes a range of IPv6 multicast addresses to the profile.
Syntax	**config mcast_filter_profile ipv6 [profile_id < value 1-60>| profile_name <name 1-32>] { profile_name <name 1-32> | [add | delete] <mcastv6_address_list>}(1)**
Description	This command allows the user to add or delete a range of multicast IPv6 addresses previously defined.
Parameters	*profile_id* – ID of the profile. Range is from *1* to *60*. *profile_name* – Provides a meaningful description for the profile. *mcast_address_list* – List of the IPv6 multicast addresses to be put in the profile. You can either specifiy a single IPv6 multicast IP address or a range of IPv6 multicast addresses.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config an IPv6 mcast_filter_ profile:

```
DGS-3700-12:5#config mcast_filter_profile ipv6 profile_id 2 add FF12::1-FF12::1
Command: config mcast_filter_profile ipv6 profile_id 2 add FF12::1

Success.

DGS-3700-12:5#
```

delete mcast_filter_profile profile_id

Purpose	This command deletes a multicast address profile.
Syntax	**delete mcast_filter_profile profile_id [ipv4|ipv6] [<value 1-60> | all]**
Description	This command deletes a multicast address profile.
Parameters	*profile_id* – ID of the profile. *all* – All multicast address profiles will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a multicast filter profile:

```
DGS-3700-12:5#delete mcast_filter_profile profile_id ipv4 2
Command: delete mcast_filter_profile profile_id ipv4 2

Success.

DGS-3700-12:5#delete mcast_filter_profile profile_id ipv6 2
Command: delete mcast_filter_profile profile_id ipv6 2

Success.

DGS-3700-12:5#
```

delete mcast_filter_profile profile_name

Purpose	This command deletes a multicast profile name.
Syntax	**delete mcast_filter_profile profile_name [ipv4|ipv6] <name 1-32>**
Description	This command deletes a multicast profile.
Parameters	*profile_name <name 1-32 >* – Name of the profile.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a multicast filter profile profile name:

```
DGS-3700-12:5#delete mcast_filter_profile profile_name ipv4 DG
Command: delete mcast_filter_profile profile_name ipv4 DG

Success.

DGS-3700-12:5#delete mcast_filter_profile profile_id ipv6 RG
Command: delete mcast_filter_profile profile_id ipv6 RG

Success.

DGS-3700-12:5#
```

show mcast_filter_profile

Purpose	This command displays the defined multicast address profiles.
Syntax	**show mcast_filter_profile [ipv4|ipv6] { profile_id <value 1-60> | profile_name <name 1-32>}**
Description	This command displays the defined multicast address profiles.
Parameters	*profile_id* – ID of the profile if not specified all profiles will be displayed. *profile_name <name 1-32 >* – Name of the profile if not specified all profiles will be displayed.
Restrictions	None.

Example usage:

To display a multicast filter profile:

```
DGS-3700-12:5#show mcast_filter_profile ipv4
Command: show mcast_filter_profile ipv4

Profile ID       Name         Multicast Addresses
----             ----------   --------------------------
1                 RG         234.1.1.1 - 238.244.244.244

Total Profile Count : 1

DGS-3700-12:5#
```

config limited_multicast_addr ports

Purpose	Used to configure the multicast address filtering function on a port.
Syntax	**config limited_multicast_addr [ports <portlist> | vlanid <vlanid_list>] [ipv4|ipv6] {[add | delete] [profile_id <value 1-60> | profile_name <name 1-32>] | access [permit | deny]}(1)**
Description	This 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. When the function is configured on a port, it limits the multicast group operated by the IGMP.
Parameters	*<portlist>* – A range of ports to config the multicast address filtering function. *<vlanid_list>* – A range of VLAN IDs to config the multicast address filtering function. *add* – Add a multicast address profile to a port. *delete* – Delete a multicast address profile to a port. *profile_id* – A profile to be added to or deleted from the port. *profile_name <name 1-32>* – The name of the profile. *permit* – Specifies that the packet that match the addresses defined in the profiles will be permitted. The default mode is permit. *deny* – Specifies that the packet that match the addresses defined in the profiles will be denied.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config port 1,3 to set the multicast address profile 2:

```
DGS-3700-12:5#config limited_multicast_addr ports 1,3 ipv4 add profile_id 2
Command: config limited_multicast_addr ports 1,3 ipv4 add profile_id 2

Success.

DGS-3700-12:5#
```

show limited_multicast_addr ports

Purpose	Used to show per-port Limited IP multicast address range.
Syntax	**show limited_multicast_addr [ipv4|ipv6] [ports {<portlist>} | vlanid <vlanid_list>]**
Description	This command allows you to show multicast address range by ports. When the function is configured on a port, it limits the multicast groups operated by the IGMP or MLD snooping function and layer 3 function.
Parameters	*<portlist>* – A range of ports to show the limited multicast address configuration. *<vlanid_list>* – range of VLAN IDs to show the multicast address configuration.
Restrictions	None.

Example usage:

To show a limited multicast address range:

```
DGS-3700-12:5#show limited_multicast_addr ipv4 ports 1,3
Command: show limited_multicast_addr ipv4 ports 1,3

Port    : 1
Access  : Deny

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          RG                               234.1.1.1 - 238.244.244.244


Port    : 3
Access  : Deny

Profile ID Name                            Multicast Addresses
---------- ------------------------------- -------------------------------
2          TG


DGS-3700-12:5#
```

config max_mcast_group ports

Purpose	This command configures the maximum number of multicast groups that a port can join.
Syntax	**config max_mcast_group [ipv4|ipv6] [ports <portlist> | vlanid <vlanid_list] max_group [<value 1-1024> | infinite]}(1)**
Description	This command configures the maximum number of multicast groups that a port can join.
Parameters	*<portlist>* – A range of ports to config the max_mcast_group. *<vlanid_list>* – A range of VLAN IDs to config the max_mcast_group. *max_group* – Specifies the maximum number of the multicast groups. The range is from *1* to *1024* or infinite. Infinite is the default setting.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the maximum number of multicast groups:

```
DGS-3700-12:5#config max_mcast_group ipv4 ports 1,3 max_group 100
Command: config max_mcast_group ipv4 ports 1,3 max_group 100

Success.

DGS-3700-12:5#
```

show max_mcast_group ports

Purpose	This command display the max number of multicast groups that a port can join.
Syntax	**show max_mcast_group [ipv4|ipv6] [ports <portlist>} | vlanid <vlanid_list >]**
Description	This command is used to display the max number of multicast groups that a port can join.
Parameters	*<portlist>* – A range of ports to display the max number of multicast groups. *<vlanid_list>* – A range of VLAN IDs to display the max number of multicast groups.
Restrictions	None.

Example usage:

To display the maximum number of multicast groups:

```
DGS-3700-12:5#show max_mcast_group ipv4 ports 1,3
Command: show max_mcast_group ipv4 ports 1,3

Port      Max Multicast Group Number
------    ---------------------------
1         100
3         100

Total Entries: 2

DGS-3700-12:5#
```

11

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	Parameters
config ports	[<portlist>| all] {medium_type[fiber|copper]} { speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full{master|slave}] | flow_control [enable | disable] | learning [enable | disable]| state [enable | disable] | [description <desc 1-32 > | clear_description]}(1)
show ports	{[<portlist>]} {[description | err_disabled]}
enable jumbo_frame	
disable jumbo_frame	
show jumbo_frame	

Each command is listed, in detail, in the following sections.

config ports

Purpose

Used to configure the Switch's port settings.

Syntax

config ports [<portlist> | all] {medium_type[fiber|copper]}{speed [auto | 10_half | 10_full | 100_half | 100_full | 1000_full {master|slave}] | flow_control [enable | disable] | learning [enable | disable] | state [enable | disable] | [description <desc 1-32> | clear_description]}(1)

Description

This command allows for the configuration of the Switch's Ethernet ports. Only the ports listed in the *<portlist>* will be affected.

Parameters

all – Configure all ports on the Switch.

<portlist> – Specifies a port or range of ports to be configured.

speed – Allows the user to adjust the speed for a port or range of ports. The user has a choice 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. Gigabit ports are statically set to 1000 and cannot be set to slower speeds. When setting port speed to 1000_full, user should specify master or slave mode for 1000-based TX interface, and leave the 1000_full without any master or slave setting for other interfaces.
- *[half* | *full]* – Configures the specified range of ports as either full-duplex or half-duplex.

flow_control [enable | *disable]* – Enable or disable flow control for the specified ports.

learning [enable | *disable]* – Enables or disables the MAC address learning on the specified range of ports.

medium_type – Specify the medium type while the configured ports are combo ports. It's an optional parameter for configuring medium type combo ports. For no combo ports, user does not need to specify medium_type in the commands.

state [enable | *disable]* – Enables or disables the specified range of ports.

description – Enter an alphanumeric string of no more than 32 characters to describe a selected port interface.

clear description – To clear the description.

Restrictions

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

NOTE: Gigabit Ethernet Fiber ports only can be set to 1000M/100M, Full, or auto.

Example usage:

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

```
DGS-3700-12:5#config ports 1-3 speed 10_full learning enable state enable flow_control
enable
Command: config ports 1-3 speed 10_full learning enable state enable flow_control
enable

Success.

DGS-3700-12:5#
```

show ports

Purpose	Used to display the current configuration of a range of ports.
Syntax	**show ports {<portlist>} { [description | err_disabled] }**
Description	This command is used to display the current configuration of a range of ports.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed. *description* – Adding this parameter to the **show ports** command indicates that a previously entered port description will be included in the display. *err_disabled* – Use this to list disabled ports including connection status and reason for being disabled.
Restrictions	None.

Example usage:

To display the configuration of all ports on a standalone switch:

```
DGS-3700-12:5#show ports
Command: show ports
Port      Port            Settings              Connection          Address
           State     Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  --------------------  ----------------------  ---------
 1        Enabled   Auto/Disabled          Link Down                Enabled
 2        Enabled   Auto/Disabled          Link Down                Enabled
 3        Enabled   Auto/Disabled          1000M/Full/None          Enabled
 4        Enabled   Auto/Disabled          Link Down                Enabled
 5        Enabled   Auto/Disabled          Link Down                Enabled
 6        Enabled   Auto/Disabled          Link Down                Enabled
 7        Enabled   Auto/Disabled          100M/Full/None           Enabled
 8        Enabled   Auto/Disabled          Link Down                Enabled
 9    (C) Enabled   Auto/Disabled          Link Down                Enabled
 9    (F) Enabled   Auto/Disabled          Link Down                Enabled
 10   (C) Enabled   Auto/Disabled          Link Down                Enabled
 10   (F) Enabled   Auto/Disabled          Link Down                Enabled
 11   (C) Enabled   Auto/Disabled          Link Down                Enabled
 11   (F) Enabled   Auto/Disabled          Link Down                Enabled
 12   (C) Enabled   Auto/Disabled          Link Down                Enabled
 12   (F) Enabled   Auto/Disabled          Link Down                Enabled

Notes:(F)indicates fiber medium and (C)indicates copper medium in a combo port

DGS-3700-12:5#
```

Example usage:

To display the configuration of all ports on a standalone switch, with description.

```
DGS-3700-12:5#show ports description
Command: show ports description

 Port      Port            Settings             Connection          Address
           State     Speed/Duplex/FlowCtrl  Speed/Duplex/FlowCtrl   Learning
 -------  --------  --------------------  ---------------------  ---------
 1        Enabled   Auto/Disabled          Link Down              Enabled
           Description:
 2        Enabled   Auto/Disabled          Link Down              Enabled
           Description:
 3        Enabled   Auto/Disabled          1000M/Full/None        Enabled
           Description:
 4        Enabled   Auto/Disabled          Link Down              Enabled
           Description:
 5        Enabled   Auto/Disabled          Link Down              Enabled
           Description:
 6        Enabled   Auto/Disabled          Link Down              Enabled
           Description:
 7        Enabled   Auto/Disabled          100M/Full/None         Enabled
           Description:
 8        Enabled   Auto/Disabled          Link Down              Enabled
           Description:

DGS-3700-12:5#
```

NOTE: Connection status displays the following status: Link Down, Speed/Duplex/FlowCtrl (link up), or Err-Disabled.

Example usage:

To display disabled ports including connection status and reason for being disabled on a standalone switch:

```
DGS-3700-12:5#show ports err_disabled
Command: show ports err_disabled

 Port    Port      Connection Status      Reason
         State
 -----   --------  --------------------  ---------------

DGS-3700-12:5#
```

enable jumbo_frame

Purpose	Used to enable the jumbo frame function on the Switch.
Syntax	**enable jumbo_frame**
Description	This command will allow ethernet frames larger than 1536 bytes to be processed by the Switch. The maximum size of the jumbo frame may not exceed 13312 Bytes tagged.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the jumbo frame:

```
DGS-3700-12:5#enable jumbo_frame
Command: enable jumbo_frame

The maximum size of jumbo frame is 13312 bytes.
Success.

DGS-3700-12:5#
```

disable jumbo_frame

Purpose	Used to disable the jumbo frame function on the Switch.
Syntax	**disable jumbo_frame**
Description	This command will disable the jumbo frame function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the jumbo frame:

```
DGS-3700-12:5#disable jumbo_frame
Command: disable jumbo_frame

Success.

DGS-3700-12:5#
```

show jumbo_frame

Purpose	Used to show the status of the jumbo frame function on the Switch.
Syntax	**show jumbo_frame**
Description	This command will show the status of the jumbo frame function on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the jumbo frame status currently configured on the Switch:

```
DGS-3700-12:5#show jumbo_frame
Command: show jumbo_frame

Jumbo Frame State  : Disabled
Maximum Frame Size : 1536 Bytes


DGS-3700-12:5#
```

12

ARP COMMANDS

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

Command	Parameters
create arpentry	<ipaddr> <macaddr>
config arpentry	<ipaddr> <macaddr>
delete arpentry	[<ipaddr> | all]
show arpentry	{ipif <ipif_name 12> | ipaddress <ipaddr> | static}
config arp_aging time	<value 0-65535>
clear arptable	

Each command is listed, in detail, in the following sections.

create arpentry

Purpose	Used to make a static entry into the ARP table.
Syntax	**create arpentry <ipaddr> <macaddr>**
Description	This command is used to enter an IP address and the corresponding MAC address into the Switch's ARP table.
Parameters	*<ipaddr>* – The IP address of the end node or station. *<macaddr>* – The MAC address corresponding to the IP address above.
Restrictions	Only Administrator and Operator-level users can issue this command. The Switch supports up to 255 static ARP entries.

Example usage:

To create a static arp entry for the IP address 10.48.74.121 and MAC address 00:50:BA:00:07:36:

```
DGS-3700-12:5#create arpentry 10.48.74.121 00-50-BA-00-07-36
Command: create arpentry 10.48.74.121 00-50-BA-00-07-36

Success.

DGS-3700-12:5#
```

config arpentry

Purpose	Used to configure a static entry in the ARP table.
Syntax	**config arpentry <ipaddr> <macaddr>**
Description	This command is used to configure a static entry in the ARP Table. The user may specify the IP address and the corresponding MAC address of an entry in the Switch's ARP table.
Parameters	*<ipaddr>* – The IP address of the end node or station. *<macaddr>* – The MAC address corresponding to the IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure a static arp entry for the IP address 10.48.74.12 and MAC address 00:50:BA:00:07:36:

```
DGS-3700-12:5#config arpentry 10.48.74.12 00-50-BA-00-07-36
Command: config arpentry 10.48.74.12 00-50-BA-00-07-36

Success.

DGS-3700-12:5#
```

delete arpentry

Purpose	Used to delete a static entry into the ARP table.
Syntax	**delete arpentry [<ipaddr> | all]**
Description	This command is used to delete a static ARP entry, made using the **create arpentry** command above, by specifying either the IP address of the entry or all. Specifying *all* clears the Switch's ARP table.
Parameters	*<ipaddr>* – The IP address of the end node or station. *all* – Deletes all ARP entries.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an entry of IP address 10.48.74.121 from the ARP table:

```
DGS-3700-12:5#delete arpentry 10.48.74.121
Command: delete arpentry 10.48.74.121

Success.

DGS-3700-12:5#
```

config arp_aging time

Purpose	Used to configure the age-out timer for ARP table entries on the Switch.
Syntax	**config arp_aging time <value 0-65535>**
Description	This 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 set in the range of *0* to *65535* minutes with a default setting of *20* minutes.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ARP aging time:

```
DGS-3700-12:5#config arp_aging time 30
Command: config arp_aging time 30

Success.

DGS-3700-12:5#
```

show arpentry

Purpose	Used to display the ARP table.
Syntax	**show arpentry {ipif <ipif_name 12> | ipaddress <ipaddr> | static }**
Description	This command is used to display the current contents of the Switch's ARP table.
Parameters	*ipif <ipif_name 12>* – The name of the IP interface the end node or station for which the ARP table entry was made, resides on. *ipaddress <ipaddr>* – The network address corresponding to the IP interface name above. *static* – Displays the static entries to the ARP table.
Restrictions	None.

Example usage:

To display the ARP table**:**

```
DGS-3700-12:5#show arpentry
Command: show arpentry

ARP Aging Time : 20

Interface       IP Address        MAC Address         Type
--------------  ---------------   -----------------   ---------------
System          10.0.0.0          FF-FF-FF-FF-FF-FF   Local/Broadcast
System          10.24.73.21       00-01-02-03-04-00   Local
System          10.48.74.121      00-50-BA-00-07-36   Static
System          10.255.255.255    FF-FF-FF-FF-FF-FF   Local/Broadcast

Total Entries: 4


DGS-3700-12:5#
```

clear arptable

Purpose	Used to remove all dynamic ARP table entries.
Syntax	**clear arptable**
Description	This 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 and Operator-level users can issue this command.

Example usage:

To remove dynamic entries in the ARP table:

```
DGS-3700-12:5#clear arptable
Command: clear arptable

Success.

DGS-3700-12:5#
```

13 DHCP RELAY

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

Command	Parameters
config dhcp_relay	{hops <value 1-16> | time <sec 0-65535>}(1)
config dhcp_relay add ipif	<ipif_name 12> <ipaddr>
config dhcp_relay delete ipif	<ipif_name 12> <ipaddr>
config dhcp_relay option_60 add	string <mutiword 255> relay <ipaddr> [exact-match|partial-match]
config dhcp_relay option_60 delete	[string <mutiword 255> {relay <ipaddr>} |ipaddress <ipaddr>| all |default {<ipaddr>}]
show dhcp_relay option_60	{[string<mutiword 255>| ipaddress <ipaddr>| default]}
config dhcp_relay option_60 default	[relay <ipaddr> |mode [relay|drop]]
config dhcp_relay option_60 state	[enable |disable]
config dhcp_relay option_61 add	[mac_address <macaddr> |string <desc_long 255>] [relay <ipaddr>| drop]
show dhcp_relay option_61	
config dhcp_relay option_61 delete	[mac_address <macaddr> | string <desc_long 255>|all]
config dhcp_relay option_61 default	[relay <ipaddr>|drop]
config dhcp_relay option_61 state	[enable|disable]
config dhcp_relay option_82 state	[enable | disable]
config dhcp_relay option_82 check	[enable | disable]
config dhcp_relay option_82 policy	[replace | drop | keep]
show dhcp_relay	{ipif <ipif_name 12>}
enable dhcp_relay	
disable dhcp_relay	

Each command is listed in detail in the following sections.

config dhcp_relay

Purpose	Used to configure the DHCP/BOOTP relay feature of the switch.
Syntax	**config dhcp_relay {hops <value 1-16> | time <sec 0-65535>}(1)**
Description	This command is used to configure the DHCP/BOOTP relay feature.
Parameters	*hops <value 1-16>* – Specifies the maximum number of relay agent hops that the DHCP packets can cross. *time <sec 0-65535>* – If this time is exceeded, the Switch will relay the DHCP packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config DHCP relay:

```
DGS-3700-12:5#config dhcp_relay hops 2 time 23
Command: config dhcp_relay hops 2 time 23

Success.

DGS-3700-12:5#
```

config dhcp_relay add ipif

Purpose	Used to add an IP destination address to the switch's DHCP/BOOTP relay table.
Syntax	**config dhcp_relay add ipif <ipif_name 12> <ipaddr>**
Description	This command adds an IP address as a destination to forward (relay) DHCP/BOOTP relay packets to.
Parameters	*<ipif_name 12>* – The name of the IP interface in which DHCP relay is to be enabled. *<ipaddr>* – The DHCP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add an IP destination to the DHCP relay table:

```
DGS-3700-12:5#config dhcp_relay add ipif System 10.58.44.6
Command: config dhcp_relay add ipif System 10.58.44.6

Success.

DGS-3700-12:5#
```

config dhcp_relay delete ipif

Purpose	Used to delete one or all IP destination addresses from the Switch's DHCP/BOOTP relay table.
Syntax	**config dhcp_relay delete ipif <ipif_name 12> <ipaddr>**
Description	This command is used to delete an IP destination addresses in the Switch's DHCP/BOOTP relay table.
Parameters	*<ipif_name 12>* – The name of the IP interface that contains the IP address below. *<ipaddr>* – The DHCP server IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IP destination from the DHCP relay table:

```
DGS-3700-12:5#config dhcp_relay delete ipif System 10.58.44.6
Command: config dhcp_relay delete ipif System 10.58.44.6

Success.

DGS-3700-12:5#
```

config dhcp_relay option_60 state

Purpose	This command is used to configure the state of DHCP relay agent information option 82 of the switch. Used to config dhcp_relay opton_60 state.
Syntax	**config dhcp_relay option_60 state [enable |disable]**
Description	This command decides whether dhcp_relay will process the DHCP option 60 or not. When option_60 is enabled, if the packet does not have option 60, then the relay servers cannot be determined based on option 60. The relay servers will be determined based on either option 61 or per IPIF configured servers. If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.
Parameters	*enable* – Enables the fuction. *disable* – Disables the fuction.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure DHCP relay option 60 state:

```
DGS-3700-12:5#config dhcp_relay option_60 state enable
Command: config dhcp_relay option_60 state enable

Success.

DGS-3700-12:5#
```

config dhcp_relay option_60 add

Purpose	This command is used to add a entry for dhcp_relay option_60
Syntax	**config dhcp_relay option_60 add string <mutiword 255> relay <ipaddr> [exact-match|partial-match]**
Description	This command configures the option 60 relay rules. Note that different strings can be specified with the same relay server, and the same string can be specified with multiple relay servers. The system will relay the packet to all the matching servers.
Parameters	*exact-match* – The option 60 string in the packet must fully match the specified string. *partial-match* – The option 60 string in the packet only need partial match with the specified string. *string* – The specified string. *ipaddress* – Specify a relay server IP address.
Restrictions	Only Administrator can issue this command.

Example usage:

To configure a new dhcp relay with option 60:

```
DGS-3700-12:5#config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-
match
Command: config dhcp_relay option_60 add string "abc" relay 10.90.90.1 exact-match

Success.

DGS-3700-12:5#
```

config dhcp_relay option_60 default

Purpose	This command is used to configure dhcp_relay option_60 default relay servers
Syntax	**config dhcp_relay option_60 default [relay <ipaddr> |mode[relay|drop]]**
Description	When there are no matching servers found for the packet, based on option 60, the relay servers will be determined by the default relay server settings. When drop is specified, the packet with no matching rules found will be dropped without further process. If the setting states no- drop, then the packet will be processed further based on option 61. The final relay servers will be the union of option 60 default relay servers and the relay servers determined by option 61.
Parameters	*ipaddress* – The specified ipaadress for dhcp_relay forward. Specifies a relay server IP for the packet that has mathcing option 60 rules. *drop* – Specify to drop the packet that has no matching option 60 rules. *relay* – The packet will be relayed based on the relay rules.
Restrictions	Only Administrator can issue this command.

Example usage:

To configure the DHCP relay default option 60:

```
DGS-3700-12:5#config dhcp_relay option_60 default mode drop
Command: config dhcp_relay option_60 default mode drop

Success.

DGS-3700-12:5#
```

config dhcp_relay option_60 delete

Purpose	This command is used to delete dhcp_relay option_60 entry.
Syntax	**config dhcp_relay option_60 delete [string <mutiword 255> {relay <ipaddr>} |ipaddress <ipaddr>| all |default {<ipaddr>}]**
Description	This command can delete the entry specifed by user. When all is specified, all rules excluding the default rules are deleted
Parameters	*ipaddress* – Deletes any entry whose ipaddress is equal to the specified ipaddress. *default* – Deletes any defaut relay ipaddress if ipaddress is not specified. *drop* – Specify to drop the packet that has no matching option 60 rules. *relay* – Deletes the entry, whose string and IP address are equal to the string and IP address specified by the user. *all* – Deletes all entries, however default relay servers are excluded. *string* – Deletes all the entries whose string is equal to the string specified if the ipaddress is not specified
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the DHCP relay option 60:

```
DGS-3700-12:5#config dhcp_relay option_60 delete all
Command: config dhcp_relay option_60 delete all

Success.

DGS-3700-12:5#
```

show dhcp_relay option_60

Purpose	This command is used to show dhcp_relay option_60 entry.
Syntax	**show dhcp_relay option_60 {[string <mutiword 255>| ipaddress <ipaddr>| default]}**
Description	This command will display the dhcp_relay option_60 entry by the user specified.
Parameters	*ipaddress* – Shows the entry whose ipaddress is equal to the specified ipaddress. *default* – Shows the default behaviour of dhcp_relay option60. *string* – Shows the entry whose string is equal to the string of a specified user.
Restrictions	None.

Example usage:

To display the DHCP relay option 60:

```
DGS-3700-12:5#show dhcp_relay option_60
Command: show dhcp_relay option_60

Default Processing Mode: Drop

Default Servers:

Matching Rules:

String                          Match Type            IP Address
-------                         -----------           ---------
abc                             Exact Match           10.90.90.1

Total Entries : 1

DGS-3700-12:5#
```

config dhcp_relay option_61 state

Purpose	This command is used to configure the DHCP relay option 61 state.
Syntax	**config dhcp_relay option_61 state [enable|disable]**
Description	This command decides whether dhcp_relay will process the DHCP option 61 or not. When option_61 is enabled, if the packet does not have option 61, then the relay servers cannot be determined based on option 61. If the relay servers are determined based on option 60 or option 61, then per IPIF configured servers will be ignored. If the relay servers are not determined either by option 60 or option 61, then per IPIF configured servers will be used to determine the relay servers.
Parameters	*enable* – Enables the fuction dhcp_relay use option_61 ruler to relay dhcp packet. disable – Disables the fuction dhcp_relay use option_61 ruler to relay dhcp packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the state of DHCP relay option 61:

```
DGS-3700-12:5#config dhcp_relay option_61 state enable
Command: config dhcp_relay option_61 state enable

Success.

DGS-3700-12:5#
```

config dhcp_relay option_61 add

Purpose	This command is used to add a rule for dhcp_relay option_61.
Syntax	**config dhcp_relay option_61 add [mac_address <macaddr> |string <desc 255>] [relay <ipaddr>| drop]**
Description	This command adds a rule to determine the relay server based on option 61. The matched rule can be based on either the MAC address or a user-specified string. Only one relay server can be specified for a MAC-address or a string. If the relay servers are determined based on option 60, and one relay server is determined based on option 61, the final relay servers will be the union of these two sets of the servers.
Parameters	*mac_address* – The client's client-ID which is the hardware address of client. *string* – The client's client-ID,which is specified by administrator. *relay* – Specify to relay the packet to a IP address. *drop* – Specify to drop the packet.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the DHCP relay option 61:

```
DGS-3700-12:5#config dhcp_relay option_61 add mac_address 00-01-22-33-44-55 drop
Command: config dhcp_relay option_61 add mac_address 00-01-22-33-44-55 drop

Success.

DGS-3700-12:5#
```

config dhcp_relay option_61 default

Purpose	This command is used to determine the default ruler for option 61.
Syntax	**config dhcp_relay option_61 default [relay <ipaddr>|drop]**
Description	This command is used to determine the rule to process those packets that have no option 61 matching rules. The default default-rule is drop.
Parameters	*relay* – Specifies to relay the packet that has no option 61 matching rules to an IP address. *drop* – Specifies to drop the packet that has no option 61 matching rules.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the DHCP relay option 61 default:

```
DGS-3700-12:5#config dhcp_relay option_61 default drop
Command: config dhcp_relay option_61 default drop

Success.

DGS-3700-12:5#
```

config dhcp_relay option_61 delete

Purpose	This command is used to delete an option 61 rule.
Syntax	**config dhcp_relay option_61 delete [mac_address <macaddr> | string <desc 255>|all]**
Description	This command is used to delete an option 61 rule.
Parameters	*mac_address* – The entry with the specified MAC address will be deleted. *string* – The entry with the specified string will be deleted. *all* – All rules excluding the default rule will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the DHCP relay option 61 rules:

```
DGS-3700-12:5# config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55
Command: config dhcp_relay option_61 delete mac_address 00-11-22-33-44-55

Success

DGS-3700-12:5#
```

show dhcp_relay option_61

Purpose	This command displays DHCP relay option 61.
Syntax	**show dhcp_relay option_61**
Description	This command displays DHCP relay option 61.
Parameters	None.
Restrictions	None.

Example usage:

To display the DHCP relay option 61:

```
DGS-3700-12:5#show dhcp_relay option_61
Command: show dhcp_relay option_61

Default Relay Rule:Drop

Matching Rules:

Client-ID                    Type              Relay Rule
-----------                  ----              ---------
00-01-22-33-44-55            MAC Address       Drop

Total Entries : 1

DGS-3700-12:5#
```

config dhcp_relay option_82 state

Purpose	Used to configure the state of DHCP relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 state [enable | disable]**
Description	This command is used to configure the state of DHCP relay agent information option 82 of the switch.
Parameters	*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 and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 state:

```
DGS-3700-12:5#config dhcp_relay option_82 state enable
Command: config dhcp_relay option_82 state enable

Success.

DGS-3700-12:5#
```

config dhcp_relay option_82 check

Purpose	Used to configure the checking mechanism of DHCP relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 check [enable | disable]**
Description	This command is used to configure the checking mechanism of DHCP/BOOTP relay agent information option 82 of the switch.
Parameters	*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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 check:

```
DGS-3700-12:5#config dhcp_relay option_82 check enable
Command: config dhcp_relay option_82 check enable

Success.

DGS-3700-12:5#
```

config dhcp_relay option_82 policy

Purpose	Used to configure the reforwarding policy of relay agent information option 82 of the switch.
Syntax	**config dhcp_relay option_82 policy [replace | drop | keep]**
Description	This command is used to configure the reforwarding policy of DHCP relay agent information option 82 of the switch.
Parameters	*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.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure DHCP relay option 82 policy:

```
DGS-3700-12:5#config dhcp_relay option_82 policy replace
Command: config dhcp_relay option_82 policy replace

Success.

DGS-3700-12:5#
```

show dhcp_relay

Purpose	Used to display the current DHCP/BOOTP relay configuration.
Syntax	**show dhcp_relay {ipif <ipif_name 12>}**
Description	This command will display the current DHCP relay configuration for the Switch, or if an IP interface name is specified, the DHCP relay configuration for that IP interface.
Parameters	*ipif <ipif_name 12>* – The name of the IP interface for which to display the current DHCP relay configuration.
Restrictions	None.

Example usage:

To show the DHCP relay configuration:

```
DGS-3700-12:5#show dhcp_relay
Command: show dhcp_relay

DHCP/Bootp Relay Status         : Disabled
DHCP/Bootp Hops Count Limit     : 2
DHCP/Bootp Relay Time Threshold : 23
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace

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


DGS-3700-12:5#
```

Example usage:

To show a single IP destination of the DHCP relay configuration:

```
DGS-3700-12:5#show dhcp_relay ipif System
Command: show dhcp_relay ipif System

DHCP/Bootp Relay Status         : Disabled
DHCP/Bootp Hops Count Limit     : 2
DHCP/Bootp Relay Time Threshold : 23
DHCP Vendor Class Identifier Option 60 State: Disabled
DHCP Client Identifier Option 61 State: Disabled
DHCP Relay Agent Information Option 82 State  : Disabled
DHCP Relay Agent Information Option 82 Check  : Disabled
DHCP Relay Agent Information Option 82 Policy : Replace

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

DGS-3700-12:5#
```

enable dhcp_relay

Purpose	Used to enable the DHCP/BOOTP relay function on the Switch.
Syntax	**enable dhcp_relay**
Description	This command is used to enable the DHCP/BOOTP relay function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable DHCP relay:

```
DGS-3700-12:5#enable dhcp_relay
Command: enable dhcp_relay

Success.

DGS-3700-12:5#
```

disable dhcp_relay

Purpose	Used to disable the DHCP/BOOTP relay function on the Switch.
Syntax	**disable dhcp_relay**
Description	This command is used to disable the DHCP/BOOTP relay function on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable DHCP relay:

```
DGS-3700-12:5#disable dhcp_relay
Command: disable dhcp_relay

Success.

DGS-3700-12:5#
```

14

OUT-OF-BAND MANAGEMNET COMMANDS

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

Command	Parameters
config out_band_ipif	{ipaddress <network_address> | state [enable |disable] | gateway <ipaddr>}(1)
show out_band_ipif	

Each command is listed, in detail, in the following sections.

config out_band_ipif

Purpose	Used to configure the out-of-band menagement settings.
Syntax	**config out_band_ipif {ipaddress <network_address> | state [enable |disable] | gateway <ipaddr>}(1)**
Description	This command is used to change out-of-band management settings. Out of Band Management is a method to manage devices while sharing the network bandwidth with other management traffic. Out of Band Management allows Management packets and ARP requests to pass between the CPU and the management interface while other packets will be dropped.
Parameters	*ipaddress <network_address>* – The IP address of the interface, the parameter must give the mask. *state [enable | disable]* – Allows users to enable or disable the IP interface. *gateway <ipaddr>* – Default gateway of out-of-band management networks.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the out_band interface:

```
DGS-3700-12:5#config out_band_ipif ipaddress 10.90.90.4/8 state enable
Command: config out_band_ipif ipaddress 10.90.90.4/8 state enable

Success.

DGS-3700-12:5#
```

show out_band_ipif

Purpose	Use to display the current configurations of special out-of-band management interface.
Syntax	**show out_band_ipif**
Description	The command is used to display the current configurations of out-of-band management interface.
Parameters	None
Restrictions	None.

Example usage:

To display the out_band interface .

```
DGS-3700-12:5#show out_band_ipif
Command: show out_band_ipif

Status                        : Enable
IP Address                    : 192.168.0.1
Subnet Mask                   : 255.255.255.0
GateWay                       : 0.0.0.0
Link Status                   : LinkDown


DGS-3700-12:5#
```

15

EXTERNAL ALARM COMMANDS

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

Command	Parameters
show external_alarm	
config external_alarm	channel <value 1-4> message <sentence 1-128>

Each command is listed, in detail, in the following sections.

show external_alarm

Purpose	Used to display the current external alarm status on the Switch.
Syntax	**show external_alarm**
Description	This command is used to display the current external alarm status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current external alarm on the Switch:

```
DGS-3700-12:5#show external_alarm
Command: show external_alarm

  Channel     Status      Alarm Message
-----------   ---------   -------------------------------------
     1        Normal      External Alarm 1 Occurred!
     2        Normal      External Alarm 2 Occurred!
     3        Normal      External Alarm 3 Occurred!
     4        Normal      External Alarm 4 Occurred!

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

config external_alarm

Purpose	Used to configure the external alarm prompt messages on the Switch.
Syntax	**config external_alarm channel <value 1-4> message <sentence 1-128>**
Description	This command is used to set the message to be displayed on console when external alarm occurs.
Parameters	*channel* – used to select one of the 4 channels *message* – prompt message
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the external alarm on channel 1:

```
DGS-3700-12:5#config external_alarm channel 1 message Channel 1  alarm occurs
Command: config external_alarm channel 1 message Channel 1  alarm occurs

Success.

DGS-3700-12:5#
```

16

LOCAL LOOP-BACK COMMANDS

The local loop-back commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config local_loopback	ports [<portlist> | all] [mac | phy {medium_type [copper | fiber]}] [internal | external] [enable | disable]
show local_loopback	ports {<portlist>}

Each command is listed, in detail, in the following sections.

config local_loopback

Purpose	Config local loop-back is used to start or stop the internal loop-back tests on selected ports. It is also used to set or recover the external loop-back mode.
Syntax	**config local_loopback ports [<portlist> | all] [mac | phy {medium_type [copper | fiber]}] [internal | external] [enable | disable]**
Description	When internal loop-back mode is enabled, the device starts to send test packets to the port, and keeps monitoring the packets received. When internal loop-back mode is disabled, the loop-back test is terminated and the result is displayed. A port can only operate in one loop-back mode at a time. When external an loop-back mode is enabled, the MAC/PHY is set to external loop-back mode. When external loop-back mode is disabled, the MAC/PHY reverts to normal operation.
Parameters	*ports [<portlist> | all]* – The port(s) to be set. *[mac | phy]* – Select the layer on which the loop-back is performed. *medium_type* – Specify the medium on which the loop-back test is taken for combo ports. If it's not specified, by default, the loop-back test will be performed on copper medium. *[internal | external]* – The local loop-back mode. *[enable | disable]* – Select enable or disable to: **enable**: for internal loop-back, start loop-back test; for external loop-back, set port(s) to external loop-back mode. **disable**: for internal loop-back, stop loop-back test; for external loop-back, recover port(s) from external loop-back mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable internal loop-back in the PHY layer on copper port 9:

```
DGS-3700-12:5#config local_loopback ports 9 phy medium_type fiber internal enable
Command: config local_loopback ports 9 phy medium_type fiber internal enable

Success.

DGS-3700-12:5#
```

show local_loopback

Purpose	Used to display local loop-back configurations on the Switch.
Syntax	**show local_loopback ports {<portlist>}**
Description	This command is used to display local loop-back configurations on the Switch.
Parameters	*ports [<portlist>*	*all]* – The port(s) to be set.
Restrictions	None.

Example usage:

To show loop-back configuration:

```
DGS-3700-12:5#show local_loopback ports 1-9
Command: show local_loopback ports 1-9

 Port       Loopback Mode
------     ---------------------
  1         None
  2         None
  3         None
  4         None
  5         None
  6         None
  7         None
  8         None
  9         Internal PHY Fiber

DGS-3700-12:5#
```

17

MAC NOTIFICATION COMMANDS

The MAC notification commands in the Command Line Interface (CLI) are listed, in the following table, along with their appropriate parameters.

Command	Parameters
enable mac_notification	
disable mac_notification	
config mac_notification	{interval <int 1-2147483647> | historysize <int 1-500>}(1)
config mac_notification ports	[<portlist> | all] [enable | disable]
show mac_notification	
show mac_notification ports	{<portlist>}

Each command is listed, in detail, in the following sections.

enable mac_notification

Purpose	Used to enable global MAC address table notification on the Switch.
Syntax	**enable mac_notification**
Description	This command is used to enable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MAC notification without changing basic configuration:

```
DGS-3700-12:5#enable mac_notification
Command: enable mac_notification

Success.

DGS-3700-12:5#
```

disable mac_notification

Purpose	Used to disable global MAC address table notification on the Switch.
Syntax	**disable mac_notification**
Description	This command is used to disable MAC address notification without changing configuration.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable MAC notification without changing basic configuration:

```
DGS-3700-12:5#disable mac_notification
Command: disable mac_notification

Success.

DGS-3700-12:5#
```

config mac_notification

Purpose	Used to configure MAC address notification.
Syntax	**config mac_notification {interval <int 1-2147483647> | historysize <int 1-500>}(1)**
Description	This command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*interval <sec 1-2147483647>* – The time in seconds between notifications. The user may choose an interval between 1 and 2,147,483,647 seconds. *historysize <1-500>* – The maximum number of entries listed in the history log used for notification.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

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

```
DGS-3700-12:5#config mac_notification interval 1 historysize 500
Command: config mac_notification interval 1 historysize 500

Success.

DGS-3700-12:5#
```

config mac_notification ports

Purpose	Used to configure MAC address notification status settings.
Syntax	**config mac_notification ports [<portlist> | all] [enable | disable]**
Description	This command is used to monitor MAC addresses learned and entered into the FDB.
Parameters	*<portlist>* – Specify 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 and Operator-level users can issue this command.

Example usage:

To enable port 7 for MAC address table notification:

```
DGS-3700-12:5#config mac_notification ports 7 enable
Command: config mac_notification ports 7 enable

Success.

DGS-3700-12:5#
```

show mac_notification

Purpose	Used to display the Switch's MAC address table notification global settings.
Syntax	**show mac_notification**
Description	This 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-3700-12:5#show mac_notification
Command: show mac_notification

Global Mac Notification Settings


State          : Enabled
Interval       : 1
History Size   : 1

DGS-3700-12:5#
```

show mac_notification ports

Purpose	Used to display the Switch's MAC address table notification status settings.
Syntax	**show mac_notification ports {<portlist>}**
Description	This 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-3700-12:5#show mac_notification ports
Command: show mac_notification ports

Port #  MAC Address Table Notification State
------  ------------------------------------
1                   Disabled
2                   Disabled
3                   Disabled
4                   Disabled
5                   Disabled
6                   Disabled
7                   Disabled
8                   Disabled
9                   Disabled
10                  Disabled
11                  Disabled
12                  Disabled
```

18

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, AuthNoPriv or AuthPriv
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	Parameters
create snmp user	<user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16 > | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}
delete snmp user	<user_name 32>
show snmp user	
create snmp view	<view_name 32> <oid> view_type [included | excluded]
delete snmp view	<view_name 32> [all | oid]
show snmp view	{<view_name 32>}
create snmp community	<community_string 32> view <view_name 32> [read_only | read_write]
delete snmp community	<community_string 32>
show snmp community	{<community_string 32>}
config snmp engineID	<snmp_engineID 10-64>
show snmp engineID	
create snmp group	<groupname 32> [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}(1)
delete snmp group	<groupname 32>
show snmp groups	
create snmp host	[host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv]] <auth_string 32>

Command	Parameters
delete snmp host	<ipaddr>
delete snmp v6host	<ipv6addr>
show snmp host	{<ipaddr>}
show snmp v6host	{<ipv6addr>}
create trusted_host	[<ipaddr> | network <network_address>]
delete trusted_host	[ipaddr <ipaddr> | network <network_address> | all]
show trusted_host	{<network_address>}
enable snmp traps	
enable snmp authenticate_traps	
show snmp traps	
disable snmp traps	
disable snmp authenticate_traps	
config snmp system_contact	<sw_contact>
config snmp system_location	<sw_location>
config snmp system_name	<sw_name>
enable snmp	
disable snmp	

Each command is listed, in detail, in the following sections.

create snmp user

Purpose	Used to create a new SNMP user and adds the user to an SNMP group that is also created by this command.
Syntax	**create snmp user <user_name 32> <groupname 32> {encrypted [by_password auth [md5 <auth_password 8-16> | sha <auth_password 8-20>] priv [none | des <priv_password 8-16>] | by_key auth [md5 <auth_key 32-32> | sha <auth_key 40-40>] priv [none | des <priv_key 32-32>]]}**
Description	This command is used to create a new SNMP user and adds the user to an SNMP group that is also created by this command. SNMP ensures: 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.
Parameters	*<user_name 32>* – An alphanumeric name of up to 32 characters that will identify the new SNMP user. *<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. *encrypted* – Allows the user to choose a type of authorization for authentication using SNMP. The user may choose: *by_password* – Requires the SNMP user to enter a password for authentication and privacy. The password is defined by specifying the auth_password below. This method is recommended.

create snmp user

by_key – Requires the SNMP user to enter a encryption key for authentication and privacy. The key is defined by specifying the key in hex form below. This method is not recommended.

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 will be used. md5 may be utilized by entering one of the following:

- <*auth password 8-16*> - An alphanumeric string of between 8 and 16 characters that will be used to authorize the agent to receive packets for the host.
- <*auth_key 32-32*> - Enter an alphanumeric string of exactly 32 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.

sha – Specifies that the HMAC-SHA-96 authentication level will be used.

- <*auth password 8-20*> - An alphanumeric string of between 8 and 20 characters that will be used to authorize the agent to receive packets for the host.
- <*auth_key 40-40*> - Enter an alphanumeric string of exactly 40 characters, in hex form, to define the key that will be used to authorize the agent to receive packets for the host.

priv – Adding the priv (privacy) parameter will allow for encryption in addition to the authentication algorithm for higher security. The user may choose:

des – Adding this parameter will allow for a 56-bit encryption to be added using the DES-56 standard using:

- <*priv_password 8-16*> - An alphanumeric string of between 8 and 16 characters that will be used to encrypt the contents of messages the host sends to the agent.
- <*priv_key 32-32*> - Enter an alphanumeric key string of exactly 32 characters, in hex form, that will be used to encrypt the contents of messages the host sends to the agent.

none – Adding this parameter will add no encryption.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To create an SNMP user on the Switch:

```
DGS-3700-12:5#create snmp user dlink default encrypted by_password auth md5 canadian
priv none
Command: create snmp user dlink default encrypted by_password auth md5 canadian priv
none

Success.

DGS-3700-12:5#
```

delete snmp user

Purpose	Used to remove an SNMP user from an SNMP group and also to delete the associated SNMP group.
Syntax	**delete snmp user <user_name 32>**
Description	This command is used to remove an SNMP user from its SNMP group and then deletes the associated SNMP group.
Parameters	*<user_name 32>* – An alphanumeric string of up to 32 characters that identifies the SNMP user that will be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously entered SNMP user on the Switch:

```
DGS-3700-12:5#delete snmp user dlink
Command: delete snmp user dlink

Success.

DGS-3700-12:5#
```

show snmp user

Purpose	Used to display information about each SNMP username in the SNMP group username table.
Syntax	**show snmp user**
Description	This command is used to display 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-3700-12:5#show snmp user
Command: show snmp user

Username      Group Name         VerAuthPriv
--------      -------------      -----------
initial        initial           V3 NoneNone
Total Entries: 1

DGS-3700-12:5#
```

create snmp view

Purpose	Used to assign views to community strings to limit which MIB objects and SNMP manager can access.
Syntax	**create snmp view <view_name 32> <oid> view_type [included | excluded]**
Description	This command is used to assign views to community strings to limit which MIB objects an SNMP manager can access.
Parameters	*<view_name 32>* – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be created. *<oid>* – The object ID that identifies an object tree (MIB tree) that will be included or excluded from access by an SNMP manager. *view type* – Sets the view type to be: • *included* – Include this object in the list of objects that an SNMP manager can access. • *excluded* – Exclude this object from the list of objects that an SNMP manager can access.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP view:

```
DGS-3700-12:5#create snmp view dlinkview 1.3.6 view_type included
Command: create snmp view dlinkview 1.3.6 view_type included

Success.

DGS-3700-12:5#
```

delete snmp view

Purpose	Used to remove an SNMP view entry previously created on the Switch.
Syntax	**delete snmp view <view_name 32> [all | <oid>]**
Description	This command is used to remove an SNMP view previously created on the Switch.
Parameters	*<view_name 32>* – An alphanumeric string of up to 32 characters that identifies the SNMP view to be deleted. *all* – Specifies that all of the SNMP views on the Switch will be deleted. *<oid>* – The object ID that identifies an object tree (MIB tree) that will be deleted from the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a previously configured SNMP view from the Switch:

```
DGS-3700-12:5#delete snmp view dlinkview all
Command: delete snmp view dlinkview all

Success.

DGS-3700-12:5#
```

show snmp view

Purpose	Used to display an SNMP view previously created on the Switch.
Syntax	**show snmp view {<view_name 32>}**
Description	This command is used to display an SNMP view previously created on the Switch.
Parameters	*<view_name 32>* – An alphanumeric string of up to 32 characters that identifies the SNMP view that will be displayed.
Restrictions	None.

Example usage:

To display SNMP view configuration:

```
DGS-3700-12:5#show snmp view
Command: show snmp view

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

Total Entries: 8

DGS-3700-12:5#
```

create snmp community

Purpose	Used to create an SNMP community string to define the relationship between the SNMP manager and an agent. 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. An MIB view that defines the subset of all MIB objects that will be accessible to the SNMP community. *read_write* or *read_only* level permission for the MIB objects accessible to the SNMP community.
Syntax	**create snmp community <community_string 32> view <view_name 32> [read_only | read_write]**
Description	This command is used to create an SNMP community string and to assign access-limiting characteristics to this community string.
Parameters	*<community_string 32>* – An alphanumeric string of up to 32 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. *view <view_name 32>* – An alphanumeric string of up to 32 characters that is used to identify the group of MIB objects that a remote SNMP manager is allowed to access on the Switch. *read_only* – Specifies that SNMP community members using the community string created with this command can only read the contents of the MIBs on the Switch. *read_write* – Specifies that SNMP community members using the community string created with this command can read from and write to the contents of the MIBs on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the SNMP community string "dlink":

```
DGS-3700-12:5#create snmp community dlink view ReadView read_write
Command: create snmp community dlink view ReadView read_write

Success.

DGS-3700-12:5#
```

delete snmp community

Purpose	Used to remove a specific SNMP community string from the Switch.
Syntax	**delete snmp community <community_string 32>**
Description	This command is used to remove a previously defined SNMP community string from the Switch.
Parameters	*<community_string 32>* – An alphanumeric string of up to 32 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	Only Administrator-level users can issue this command.

Example usage:

To delete the SNMP community string "dlink":

```
DGS-3700-12:5#delete snmp community dlink
Command: delete snmp community dlink

Success.

DGS-3700-12:5#
```

show snmp community

Purpose	Used to display SNMP community strings configured on the Switch.
Syntax	**show snmp community {<community_string 32>}**
Description	This command is used to display SNMP community strings that are configured on the Switch.
Parameters	*<community_string 32>* – An alphanumeric string of up to 32 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-3700-12:5#show snmp community
Command: show snmp community

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

Total Entries: 3

DGS-3700-12:5#
```

config snmp engineID

Purpose	Used to configure a name for the SNMP engine on the Switch.
Syntax	**config snmp engineID <snmp_engineID 10-64>**
Description	This command is used to configure a name for the SNMP engine on the Switch.
Parameters	*<config snmp_engineID>* – An alphanumeric string that will be used to identify the SNMP engine on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To give the SNMP agent on the Switch the name "0035636666":

```
DGS-3700-12:5#config snmp engineID 0035636666
Command: config snmp engineID 0035636666

Success.

DGS-3700-12:5#
```

show snmp engineID

Purpose	Used to display the identification of the SNMP engine on the Switch.
Syntax	**show snmp engineID**
Description	This command is used to display the identification of the SNMP engine on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display the current name of the SNMP engine on the Switch:

```
DGS-3700-12:5#show snmp engineID
Command: show snmp engineID

SNMP Engine ID : 800000ab03000102030400

DGS-3700-12:5#
```

create snmp group

Purpose	Used 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]] {read_view <view_name 32> | write_view <view_name 32> | notify_view <view_name 32>}(1)**
Description	This command is used to create a new SNMP group, or a table that maps SNMP users to SNMP views.
Parameters	*<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with. *v1* – Specifies that SNMP version 1 will 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 will 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 will 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. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. *read_view* – Specifies that the SNMP group being created can request SNMP messages. *write_view* – Specifies that the SNMP group being created has write privileges. *notify_view* – Specifies that the SNMP group being created can receive SNMP trap messages generated by the Switch's SNMP agent. *<view_name 32>* – An alphanumeric string of up to 32 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-level users can issue this command.

Example usage:

To create an SNMP group named "sg1":

```
DGS-3700-12:5#create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1
notify_view v1
Command: create snmp group sg1 v3 noauth_nopriv read_view v1 write_view v1 notify_view
v1

Success.

DGS-3700-12:5#
```

delete snmp group

Purpose	Used to remove an SNMP group from the Switch.
Syntax	**delete snmp group <groupname 32>**
Description	This command is used to remove an SNMP group from the Switch.
Parameters	*<groupname 32>* – An alphanumeric name of up to 32 characters that will identify the SNMP group the new SNMP user will be associated with.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the SNMP group named "sg1".

```
DGS-3700-12:5#delete snmp group sg1
Command: delete snmp group sg1

Success.

DGS-3700-12:5#
```

show snmp groups

Purpose	Used 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	This command is used 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.
Parameters	None.
Restrictions	None.

Example usage:

To display the currently configured SNMP groups on the Switch:

```
DGS-3700-12:5#show snmp groups
Command: show snmp groups
Vacm Access Table Settings

Group    Name      : Group3
ReadView Name      : ReadView
WriteView Name     : WriteView
Notify View Name   : NotifyView
Security Model     : SNMPv3
Security Level     : NoAuthNoPriv

Group    Name      : Group4
ReadView Name      : ReadView
WriteView Name     : WriteView
Notify View Name   : NotifyView
Security Model     : SNMPv3
Security Level     : authNoPriv

Group    Name      : Group5
ReadView Name      : ReadView
WriteView Name     : WriteView
Notify View Name   : NotifyView
Security Model     : SNMPv3
Security Level     : authNoPriv

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

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

Total Entries: 5

DGS-3700-12:5#
```

create snmp host

Purpose	Used to create a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**create snmp [host <ipaddr> | v6host <ipv6addr>] [v1 | v2c | v3 [noauth_nopriv | auth_nopriv | auth_priv] <auth_string 32>]**
Description	This command is used to create a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	*<ipaddr>* – The IP address of the remote management station that will serve as the SNMP host for the Switch. *v6host* – Specifies the v6host IP address to which the trap packet will be sent. *v1* – Specifies that SNMP version 1 will 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 will 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 will be used. SNMP v3 provides secure access to

create snmp host

	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. *noauth_nopriv* – Specifies that there will be no authorization and no encryption of packets sent between the Switch and a remote SNMP manager. *auth_nopriv* – Specifies that authorization will be required, but there will be no encryption of packets sent between the Switch and a remote SNMP manager. *auth_priv* – Specifies that authorization will be required, and that packets sent between the Switch and a remote SNMP manger will be encrypted. <*auth_string 32*> – An alphanumeric string used to authorize a remote SNMP manager to access the Switch's SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create an SNMP host to receive SNMP messages:

```
DGS-3700-12:5#create snmp host 10.48.74.100 v3 auth_priv public
Command: create snmp host 10.48.74.100 v3 auth_priv public

Success.

DGS-3700-12:5#
```

delete snmp host

Purpose	Used to remove a recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**delete snmp host <ipaddr>**
Description	This command is used to delete a recipient of SNMP traps generated by the Switch's SNMP agent.
Parameters	<*ipaddr*> – The IP address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete an SNMP host entry:

```
DGS-3700-12:5#delete snmp host 10.48.74.100
Command: delete snmp host 10.48.74.100

Success.

DGS-3700-12:5#
```

show snmp host

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

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DGS-3700-12:5#show snmp host
Command: show snmp host

SNMP Host Table
Host IP Address  SNMP Version Community Name/SNMPv3 User Name
---------------  ------------  ----------------------------
10.48.76.23      V2c                    private
10.48.74.100     V3     authpriv        public

Total Entries: 2

DGS-3700-12:5#
```

show snmp v6host

Purpose	Used to display the recipient of SNMP traps generated by the Switch's SNMP agent.
Syntax	**show snmp v6host {<ipv6addr>}**
Description	This 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	<*ipv6addr*> – The IPv6 address of a remote SNMP manager that will receive SNMP traps generated by the Switch's SNMP agent.
Restrictions	None.

Example usage:

To display the currently configured SNMP hosts on the Switch:

```
DGS-3700-12:5#show snmp v6host
Command: show snmp v6host

SNMP Host Table
-----------------------------------------------------------------
Host IPv6 Address : ::C084:1
SNMP Version      : V1
Community Name/SNMPv3 User Name : 2

Total Entries: 1

DGS-3700-12:5#
```

create trusted_host

Purpose	Used to create the trusted host.
Syntax	**create trusted_host <ipaddr>**
Description	This command is used to create the trusted host. The Switch allows users to specify up to four IP addresses that are allowed to manage the Switch via in-band SNMP or TELNET based management software. These IP addresses must be members of the Management VLAN. If no IP addresses are specified, then there is nothing to prevent any IP address from accessing the Switch, provided the user knows the Username and Password.
Parameters	*<ipaddr>* – The IP address of the trusted host to be created.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the trusted host:

```
DGS-3700-12:5#create trusted_host 10.62.32.1
Command: create trusted_host 10.62.32.1

Success.
```

create trusted_host network

Purpose	Used to create the trusted host.
Syntax	**create trusted_host network <network_address>**
Description	This command is used to create the trusted host.
Parameters	*<network_address>* – IP address and netmask of the trusted host to be created.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the trusted host network.

```
DGS-3700-12:5#create trusted_host network 10.62.32.1/16
Command: create trusted_host network 10.62.32.1/16

Success.
```

show trusted_host

Purpose	Used to display a list of trusted hosts entered on the Switch using the **create trusted_host** command above.
Syntax	**show trusted_host {<network_address>}**
Description	This command is used to display a list of trusted hosts entered on the Switch using the **create trusted_host** command above.
Parameters	<network_address> – the network address to show
Restrictions	None.

Example usage:

To display the list of trust hosts:

```
DGS-3700-12:5#show trusted_host
Command: show trusted_host
```

```
Management Stations

IP Address
-----------------
10.62.32.1/32
10.62.32.1/16

Total Entries: 2
```

delete trusted_host ipaddr

Purpose	Used to delete a trusted host entry made using the **create trusted_host** command above.
Syntax	**delete trusted *host ipaddr<ipaddr>***
Description	This command is used to delete a trusted host entry made using the **create trusted_host** command above.
Parameters	*<ipaddr>* – The IP address of the trusted host.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a trusted host with an IP address 10.62.32.1:

```
DGS-3700-12:5#delete trusted_host ipaddr 10.62.32.1
Command: delete trusted_host ipaddr 10.62.32.1

Success.
```

delete trusted_host network

Purpose	Used to delete a trusted host entry made using the **create trusted_host network** command above.
Syntax	**delete trusted _host network <network_address>**
Description	This command is used to delete a trusted host entry made using the **create trusted_host network** command above.
Parameters	*<network_address>* – IP address and netmask of the trusted host network.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a trusted host network IP address 10.62.31.1/16:

```
DGS-3700-12:5#delete trusted_host network 10.62.32.1/16
Command: delete trusted_host network 10.62.32.1/16

Success.
```

delete trusted_host all

Purpose	Used to delete all trusted host entries made using the **create trusted_host ipaddr and create trusted_host network** commands above.
Syntax	**delete trusted _host all**
Description	This command is used to delete all trusted host entries made using the **create trusted_host ipaddr and create trusted_host network** commands above.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all trusted host entries:

```
DGS-3700-12:5#delete trusted_host all
Command: delete trusted_host all

Success.
```

enable snmp traps

Purpose	Used to enable SNMP trap support.
Syntax	**enable snmp traps**
Description	This command is used to enable SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable SNMP trap support on the Switch:

```
DGS-3700-12:5#enable snmp traps
Command: enable snmp traps

Success.

DGS-3700-12:5#
```

enable snmp authenticate_traps

Purpose	Used to enable SNMP authentication trap support.
Syntax	**enable snmp authenticate_traps**
Description	This command is used to enable SNMP authentication trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To turn on SNMP authentication trap support:

```
DGS-3700-12:5#enable snmp authenticate_traps
Command: enable snmp authenticate_traps

Success.

DGS-3700-12:5#
```

show snmp traps

Purpose	Used to show SNMP trap support on the Switch.
Syntax	**show snmp traps**
Description	This command is used to view the SNMP trap support status currently configured on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current SNMP trap support:

```
DGS-3700-12:5#show snmp traps
Command: show snmp traps

SNMP Traps           : Enabled
Authenticate Trap    : Enabled

DGS-3700-12:5#
```

disable snmp traps

Purpose	Used to disable SNMP trap support on the Switch.
Syntax	**disable snmp traps**
Description	This command is used to disable SNMP trap support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To prevent SNMP traps from being sent from the Switch:

```
DGS-3700-12:5#disable snmp traps
Command: disable snmp traps

Success.

DGS-3700-12:5#
```

disable snmp authenticate_traps

Purpose	Used to disable SNMP authentication trap support.
Syntax	**disable snmp authenticate_traps**
Description	This command is used to disable SNMP authentication support on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the SNMP authentication trap support:

```
DGS-3700-12:5#disable snmp authenticate_traps
Command: disable snmp authenticate_traps

Success.

DGS-3700-12:5#
```

config snmp system_contact

Purpose	Used to enter the name of a contact person who is responsible for the Switch.
Syntax	**config snmp system_contact <sw_contact>**
Description	This command is used to enter the name and/or other information to identify a contact person who is responsible for the Switch. A maximum of 255 character can be used.
Parameters	*<sw_contact>* – A maximum of 255 characters is allowed. A NULL string is accepted if there is no contact.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Switch contact to "**MIS Department II**":

```
DGS-3700-12:5#config snmp system_contact MIS Department II
Command: config snmp system_contact MIS Department II

Success.

DGS-3700-12:5#
```

config snmp system_location

Purpose	Used to enter a description of the location of the Switch.
Syntax	**config snmp system_location <sw_location>**
Description	This command is used to enter a description of the location of the Switch. A maximum of 255 characters can be used.
Parameters	*<sw_location>* – A maximum of 255 characters is allowed. A NULL string is accepted if there is no location desired.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Switch location for "HQ 5F":

```
DGS-3700-12:5#config snmp system_location HQ 5F
Command: config snmp system_location HQ 5F

Success.

DGS-3700-12:5#
```

config snmp system_name

Purpose	Used to configure the name for the Switch.
Syntax	**config snmp system_name <sw_name>**
Description	This command is used to configure the name of the Switch.
Parameters	*<sw_name>* – A maximum of 255 characters is allowed. A NULL string is accepted if no name is desired.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the Switch name for "DGS-3700-12 Switch":

```
DGS-3700-12:5#config snmp system_name DGS-3700-12 Switch
Command: config snmp system_name DGS-3700-12 Switch

Success.

DGS-3700-12:5#
```

enable snmp

Purpose	Used to enable the SNMP interface access function.
Syntax	**enable snmp**
Description	This command is used to enable the SNMP function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable snmp on the Switch:

```
DGS-3700-12:5#enable snmp
Command: enable snmp

Success.

DGS-3700-12:5#
```

disable snmp

Purpose	Used to disable the SNMP interface access function.
Syntax	**disable snmp**
Description	This command is used to disable the SNMP function. When the SNMP function is disabled, the network manager will not be able to access SNMP MIB objects. The device will not send traps or notifications to the network manager either.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable SNMP on the Switch:

```
DGS-3700-12:5#disable snmp
Command: disable snmp

Success.

DGS-3700-12:5#
```

19

TIME AND SNTP COMMANDS

The Simple Network Time Protocol (SNTP) (an adaptation of the Network Time Protocol (NTP)) commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config sntp	{primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}(1)
show sntp	
enable sntp	
disable sntp	
config time	<date ddmmmyyyy > <time hh:mm:ss >
config time_zone	{operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}
config dst	[disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_week <end_week 1-4,last> | e-day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date <start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]
show time	

Each command is listed, in detail, in the following sections.

config sntp

Purpose	Used to setup SNTP service.
Syntax	**config sntp {primary <ipaddr> | secondary <ipaddr> | poll-interval <int 30-99999>}(1)**
Description	This command is used to configure SNTP service from an SNTP server. SNTP must be enabled for this command to function (See enable sntp).
Parameters	*primary* – This is the primary server from which the SNTP information will be taken. *<ipaddr>* – The IP address of the primary server. *secondary* – This is the secondary server the SNTP information will be taken from in the event the primary server is unavailable. *<ipaddr>* – The IP address for the secondary server. *poll-interval <int 30-99999>* – This is the interval between requests for updated SNTP information. The polling interval ranges from 30 to 99,999 seconds.
Restrictions	Only Administrator and Operator-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-3700-12:5#config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30
Command: config sntp primary 10.1.1.1 secondary 10.1.1.2 poll-interval 30

Success.

DGS-3700-12:5#
```

show sntp

Purpose	Used to display the SNTP information.
Syntax	**show sntp**
Description	This command will display SNTP settings information including the source IP address, time and poll interval.
Parameters	None.
Restrictions	None.

Example usage:

To display SNTP configuration information:

```
DGS-3700-12:5#show sntp
Command: show sntp

Current Time Source      : System Clock
SNTP                     : Disabled
SNTP Primary Server      : 10.1.1.1
SNTP Secondary Server    : 10.1.1.2
SNTP Poll Interval       : 30 sec

DGS-3700-12:5#
```

enable sntp

Purpose	To enable SNTP server support.
Syntax	**enable sntp**
Description	This command will enable SNTP support. SNTP service must be separately configured (see **config sntp**). Enabling and configuring SNTP support will 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-3700-12:5#enable sntp
Command: enable sntp

Success.

DGS-3700-12:5#
```

disable sntp

Purpose	To disable SNTP server support.
Syntax	**disable sntp**
Description	This command will disable SNTP support. SNTP service must be separately configured (see **config sntp**).
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable SNTP support:

```
DGS-3700-12:5#disable sntp
Command: disable sntp

Success.

DGS-3700-12:5#
```

config time

Purpose	Used to manually configure system time and date settings.
Syntax	**config time <date ddmmmyyyy> <time hh:mm:ss>**
Description	This command will configure the system time and date settings. These will be overridden if SNTP is configured and enabled.
Parameters	*date* – Express the date using two numerical characters for the day of the month, three alphabetical characters for the name of the month, and four numerical characters for the year. For example: 03aug2003. *time* – Express 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 and Operator-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-3700-12:5#config time 30jun2003 16:30:30
Command: config time 30jun2003 16:30:30

Success.

DGS-3700-12:5#
```

config time_zone

Purpose	Used to determine the time zone used in order to adjust the system clock.
Syntax	**config time_zone {operator [+ | -] | hour <gmt_hour 0-13> | min <minute 0-59>}**
Description	This command will adjust system clock settings according to the time zone. Time zone settings will adjust SNTP information accordingly.
Parameters	*operator* – Choose to add (+) or subtract (-) time to adjust for time zone relative to GMT. *hour* – Select the number of hours different from GMT. *min* – Select the number of minutes difference added or subtracted to adjust the time zone.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure time zone settings:

```
DGS-3700-12:5#config time_zone operator + hour 2 min 30
Command: config time_zone operator + hour 2 min 30

Success.

DGS-3700-12:5#
```

config dst

Purpose	Used to enable and configure time adjustments to allow for the use of Daylight Savings Time (DST).
Syntax	**config dst [disable | repeating {s_week <start_week 1-4,last> | s_day <start_day sun-sat> | s_mth <start_mth 1-12> | s_time start_time hh:mm> | e_week <end_week 1-4,last> | e_day <end_day sun-sat> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]} | annual {s_date start_date 1-31> | s_mth <start_mth 1-12> | s_time <start_time hh:mm> | e_date <end_date 1-31> | e_mth <end_mth 1-12> | e_time <end_time hh:mm> | offset [30 | 60 | 90 | 120]}]**
Description	This command is used to enable and configure DST. When enabled this will adjust the system clock to comply with any DST requirement. DST adjustment effects system time for both manually configured time and time set using SNTP service. *disable* – Disable the DST seasonal time adjustment for the Switch. *repeating* – Using repeating mode will enable DST seasonal time adjustment. Repeating mode requires that the DST beginning and ending date be specified using a formula. For example, specify to begin DST on Saturday during the second week of April and end DST on Sunday during the last week of October. *annual* – Using annual mode will enable DST seasonal time adjustment. 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. *s_week* – Configure the week of the month in which DST begins. • *<start_week 1-4,last>* – The number of the week during the month in which DST begins where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *e_week* – Configure the week of the month in which DST ends.
Parameters	• *<end_week 1-4,last>* – The number of the week during the month in which DST ends where 1 is the first week, 2 is the second week and so on, last is the last week of the month. *s_day* – Configure the day of the week in which DST begins. • *<start_day sun-sat>* – The day of the week in which DST begins expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *e_day* – Configure the day of the week in which DST ends. • *<end_day sun-sat>* – The day of the week in which DST ends expressed using a three character abbreviation (sun, mon, tue, wed, thu, fri, sat) *s_mth* – Configure the month in which DST begins. • *<start_mth 1-12>* – The month to begin DST expressed as a number. *e_mth* – Configure the month in which DST ends. • *<end_mth 1-12>* – The month to end DST expressed as a number. *s_time* – Configure the time of day to begin DST. • *<start_time hh:mm>* – Time is expressed using a 24-hour clock, in hours and minutes.

config dst	
	e_time – Configure the time of day to end DST. • *<end_time hh:mm>* – Time is expressed using a 24-hour clock, in hours and minutes. *s_date* – Configure the specific date (day of the month) to begin DST. • *<start_date 1-31>* – The start date is expressed numerically. *e_date* – Configure the specific date (day of the month) to begin DST. • *<end_date 1-31>* – The end date is expressed numerically. *offset [30 | 60 | 90 | 120]* – Indicates number of minutes to add or to subtract during the summertime. The possible offset times are 30,60,90,120. The default value is 60.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure daylight savings time on the Switch:

```
DGS-3700-12:5#config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2
e_day wed e_mth 10 e_time 15:30 offset 30
Command: config dst repeating s_week 2 s_day tue s_mth 4 s_time 15:00 e_week 2 e_day
wed e_mth 10 e_time 15:30 offset 30

Success.

DGS-3700-12:5#
```

show time	
Purpose	Used to display the current time settings and status.
Syntax	**show time**
Description	This command will display system time and date configuration as well as display current system time.
Parameters	None.
Restrictions	None.

Example usage:

To show the time currently set on the Switch's System clock:

```
DGS-3700-12:5#show time
Command: show time

     Current Time Source  : System Clock
     Boot Time    : 3 Jan 2000  22:45:36
     Current Time : 4 Jan 2000  01:56:30
     Time Zone    : GMT +00:00
     Daylight Saving Time  : Disabled
         Offset In Minutes : 60
         Repeating    From : Apr 1st  Sun 00:00
                      To   : Oct last Sun 00:00
         Annual       From : 29 Apr 00:00
                      To   : 12 Oct 00:00

DGS-3700-12:5#
```

20

sFLOW COMMANDS

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

Command	Parameters
enable sflow	
disable sflow	
show sflow	
create sflow flow_sampler	ports [<portlist> | all] analyzer_server_id < value 1-4> { rate <value 0- 65535> | maxheadersize < value 18-256>}
config sflow flow_sampler	ports[<portlist> | all] { rate <value 0- 65535> | maxheadersize < value 18-256>}(1)
delete sflow flow_sampler	ports [<portlist> | all]
show sflow flow_sampler	
create sflow counter_poller	ports [<portlist> | all] analyzer_server_id < value 1-4> {interval [disable | <sec 20-120>]}
config sflow counter_poller	ports [<portlist> | all] interval [disable | <sec 20-120>]
delete sflow counter_poller	ports [<portlist> | all]
show sflow counter_poller	
create sflow analyzer_server	< value 1-4 > owner<name 16> { timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize < value 300-1400> }
config sflow analyzer_server	< value 1-4 > { timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize < value 300-1400>}(1)
delete sflow analyzer_server	< value 1-4 >
show sflow analyzer_server	

Each command is listed, in detail, in the following sections.

enable sflow

Purpose	Used to enable the sFlow function.
Syntax	**enable sflow**
Description	This command is used to enable the sFlow function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable sflow:

```
DGS-3700-12:5#enable sflow
Command: enable sflow

Success.

DGS-3700-12:5#
```

disable sflow

Purpose	Used to disable the sFlow function.
Syntax	**disable sflow**
Description	This command is used to disable the sFlow function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable sflow:

```
DGS-3700-12:5#disable sflow
Command: disable sflow

Success.

DGS-3700-12:5#
```

show sflow

Purpose	Used to display the sFlow function.
Syntax	**show sflow**
Description	This command is used to display the sFlow function settings on the Swicth.
Parameters	None.
Restrictions	None.

Example usage:

To display sflow:

```
DGS-3700-12:5#show sflow
Command: show sflow

 sFlow Version  : 1.00
 sFlow Address  : 10.24.73.21
 sFlow State    : Disabled

DGS-3700-12:5#
```

create sflow flow_sampler

Purpose	Used to create the sflow flow_sampler.
Syntax	**create sflow flow_sampler ports [<portlist> | all] analyzer_server_id < value 1-4> { rate <value 0- 65535> | maxheadersize < value 18-256>}**
Description	This command is used to create the sFlow flow_sampler. By configuring the sampling function for a port, a sample packet received by this port will be encapsulated and forwarded to the analyzer server at the specified interval.
Parameters	*ports* – Specifies the list of ports to be configured. *analyzer_server_id* – The analyzer_server_id specifies the ID of a server analyzer where the packet will be forwarded. *rate* – The sampling rate for packet sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate 5120. One packet will be sampled from about 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. *maxheadersize* – The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create sflow flow_sampler:

```
DGS-3700-12:5#create sflow flow_sampler ports all analyzer_server_id 1 rate 10
maxheadersize 100
Command: create sflow flow_sampler ports all analyzer_server_id 1 rate 10
maxheadersize 100

Success.

DGS-3700-12:5#
```

config sflow flow_sampler

Purpose	Used to configure the sflow flow_sampler parameters.
Syntax	**config sflow flow_sampler ports [<portlist> | all] { rate <value 0- 65535> | maxheadersize < value 18-256>}(1)**
Description	This command is used to configure the sflow flow sampler parameters. If the user wants the change the analyzer server ID, the user needs to delete the flow sampler and create a new one.
Parameters	*ports* – Specifies the list of ports to be configured. *rate* – The sampling rate for packet sampling. The configured rate value multiplied by 256 is the actual rate. For example, if the rate is 20, the actual rate is 5120. One packet will be sampled from about 5120 packets. If set to 0, the sampler is disabled. If the rate is not specified, its default value is 0. *maxheadersize* – The maximum number of leading bytes in the packet which has been sampled that will be encapsulated and forwarded to the server. If not specified, the default value is 128.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure sflow flow_sampler:

```
DGS-3700-12:5#config sflow flow_sampler ports all rate 10 maxheadersize 100
Command: config sflow flow_sampler ports all rate 10 maxheadersize 100

Success.

DGS-3700-12:5#
```

delete sflow flow_sampler

Purpose	Used to delete the sflow flow_sampler.
Syntax	**delete sflow flow_sampler ports [<portlist> | all]**
Description	This command is used to delete the sflow flow sampler that has been configured for the specified port.
Parameters	*ports* – Specifies the list of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all the sflow flow_sampler:

```
DGS-3700-12:5#delete sflow flow_sampler ports all
Command: delete sflow flow_sampler ports all

Success.

DGS-3700-12:5#
```

show sflow flow_sampler

Purpose	Used to show the sflow flow_sampler information of ports which have been created.
Syntax	**show sflow flow_sampler**
Description	This command is used to show the sFlow flow_sampler which has been configured for ports. The actual value rate is 256 times the displayed rate value. There are two types of rates. ConfigRate is configed by the user. In order to limit the number of packets sent to the CPU when the rate of traffic to the CPU is high, the sampling rate will be decreased. This is specified as the active rate.
Parameters	None.
Restrictions	None.

Example usage:

To show the sflow flow_sampler:

```
DGS-3700-12:5#show  sflow flow_sampler
Command: show  sflow flow_sampler

 Port   Analyzer Server ID   Configured Rate   Active Rate   Max Header Size
 ----   ------------------   ---------------   -----------   ---------------
 1           1                  20                80             140
 2           2                  10                40             100

Total Entries: 2

DGS-3700-12:5#
```

create sflow counter_poller

Purpose	Used to create the sflow counter_poller.
Syntax	**create sflow counter_poller ports [<portlist> | all] analyzer_server_id < value 1-4> {interval [disable | <sec 20-120>]}**
Description	This command is used to create the sflow counter_poller. With the poller function, the statistic counter information with respect to a port will be forwarded to the server at the configured interval. These counters are RFC 2233 counters.
Parameters	*ports* – Specifies the list of ports to be configured. *analyzer_server_id* – The analyzer_server_id is the id of a analyzer_server. *interval* – The maximum number of seconds between successive statistic counters information. If set to disable, the counter-poller is disabled. If interval is not specified, its default value is disable.
Restrictions	Only Administrators and Operator-level users can issue this command.

Example usage:

To create the sflow counter_poller:

```
DGS-3700-12:5#create  sflow counter_poller ports 1 analyzer_server_id 2 interval 40
Command: create  sflow counter_poller ports 1 analyzer_server_id 2 interval 40

Success.

DGS-3700-12:5#
```

config sflow counter_poller

Purpose	Used to configure the sflow counter_poller parameters.
Syntax	**config sflow counter_poller ports [<portlist> | all] interval [disable | <sec 20-120>]**
Description	This command is used to config the sflow counter_poller parameters. If the user wants the change the analyzer_server_id, he needs to delete the counter_poller and create a new one.
Parameters	*ports* – Specifies the list of ports to be configured. *interval* – The maximum number of seconds between successive statistic counter information. If set to disable, the counter-poller is disabled. If an interval is not specified, its default value is disable.
Restrictions	Only Administrators and Operator-level users can issue this command.

Example usage:

To configure the sflow counter_poller:

```
DGS-3700-12:5#config sflow counter_poller ports 1 interval 40
Command: config sflow counter_poller ports 1interval 40

Success.

DGS-3700-12:5#
```

delete sflow counter_poller

Purpose	Used to delete the sflow counter_poller.
Syntax	**delete sflow counter_poller ports [<portlist> | all]**
Description	This command is used to delete the sflow counter poller from the specified port .
Parameters	*ports* – Specifies the list of ports to be configured.
Restrictions	Only Administrators and Operator-level users can issue this command.

Example usage:

To delete the sflow counter_poller:

```
DGS-3700-12:5#delete sflow counter_poller ports 1
Command: delete sflow counter_poller ports 1

Success.

DGS-3700-12:5#
```

show sflow counter_poller

Purpose	Used to show the sflow counter_poller information of ports which have been created.
Syntax	**show sflow counter_poller**
Description	This command is used to show the sflow counter pollers which have been configured for port.
Parameters	None.
Restrictions	None.

Example usage:

To show the sflow counter_poller:

```
DGS-3700-12:5#show  sflow counter_poller
Command: show  sflow counter_poller

Port   Analyzer Server ID   Polling Interval (secs)
----   ------------------   -----------------------
 1          1                        25
 2          3                        30

Total Entries: 2

DGS-3700-12:5#
```

create sflow analyzer_server

Purpose	Used to create the analyzer_server.
Syntax	**create sflow analyzer_server < value 1-4 > owner<name 16> { timeout [<sec 1-2000000> | infinite] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize < value 300-1400> }**
Description	This command creates the analyzer server. You can specify more than one analyzer server with the same IP address but with different UDP port numbers. You can have up to four unique combinations of IP addresses and UDP port numbers.
Parameters	*owner* – The entity making use of this sflow analyzer_server. When owner is set or modified, the timeout value will become 400 automatically. *tmeout* – The length of time before the server is timed out. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted. "infinite" indicates that analyzer_server never times out. If not specified, its default value is 400. *collectoraddress* – The IP address of the analyzer_server. If not specified, the address will be 0.0.0.0 which means that the entry will be inactive. *collectorport* – The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6364. *maxdatagramsize* – The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create the sflow analyzer_server:

```
DGS-3700-12:5#create sflow analyzer_server 1 owner monitor
Command: create sflow analyzer_server 1 owner monitor

Success.

DGS-3700-12:5#
```

config sflow analyzer_server

Purpose	Used to configure the analyzer_server information .
Syntax	**config sflow analyzer_server < value 1-4 > { timeout [<sec 1-2000000> | infinte] | collectoraddress <ipaddr> | collectorport <udp_port_number 1-65535> | maxdatagramsize < value 300-1400>}(1)**
Description	This command is used to configure the receiver information. You can specify more than one collector with the same IP address if the UDP port numbers are unique.
Parameters	*timeout* – The length of time before the server is timed out. When the analyzer_server times out, all of the flow_samplers and counter_pollers associated with this analyzer_server will be deleted. "infinite" indicates that analyzer_server never times out. If not specified, its default value is 400. *collectoraddress* – The IP address of the analyzer_server. If not specified, the address will be 0.0.0.0 which means that the entry will be inactive. *collectorport* – The destination UDP port for sending the sFlow datagrams. If not specified, the default value is 6364. *maxdatagramsize* – The maximum number of data bytes that can be packed in a single sample datagram. If not specified, the default value is 1400.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the sflow analyzer_server:

```
DGS-3700-12:5#config sflow analyzer_server 2 collectoraddress 10.90.90.9
Command: config sflow analyzer_server 2 collectoraddress 10.90.90.9

Success.

DGS-3700-12:5#
```

delete sflow analyzer_server

Purpose	Used to delete the analyzer_server.
Syntax	**delete sflow analyzer_server < value 1-4 >**
Description	This command is used to delete the analyzer server.
Parameters	*value* – analyzer_server ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the sflow analyzer_server:

```
DGS-3700-12:5#delete sflow analyzer_server 2
Command: delete sflow analyzer_server 2

Success.

DGS-3700-12:5#
```

show sflow analyzer_server

Purpose	Used to show the sflow analyzer_server information.
Syntax	**show sflow analyzer_server**
Description	This command is used to show the sflow analyzer server information. The Timeout field specifies the time configured by user. The current countdown times is the current time remaining before the server timesout.
Parameters	None.
Restrictions	None.

Example usage:

To show the sflow analyzer_server:

```
DGS-3700-12:5#show sflow analyzer_server
Command: show sflow analyzer_server

 sFlow Analyzer_server Information
 -------------------------------
 Server ID             : 1
 Owner                 : monitor
 Timeout               : 400
 Current Countdown Time: 400
 Collector Address     : 10.90.90.1
 Collector Port        : 6343
 Max Datagram Size     : 1400

Total Entries: 1

DGS-3700-12:5#
```

21

D-LINK SINGLE IP MANAGEMENT COMMANDS

Simply put, D-Link Single IP Management is a concept that will stack switches together over Ethernet instead of using stacking ports or modules. Switches using D-Link Single IP Management (labeled here as SIM) must conform to the following rules:

SIM is an optional feature on the Switch and can easily be enabled or disabled. SIM grouping has no effect on the normal operation of the Switch in the user's network.

There are three classifications for switches using SIM. The **Commander Switch(CS)**, which is the master switch of the group, **Member Switch(MS)**, which is a switch that is recognized by the CS a member of a SIM group, and a **Candidate Switch(CaS)**, which is a switch that has a physical link to the SIM group but has not been recognized by the CS as a member of the SIM group.

A SIM group can only have one Commander Switch(CS).

All switches in a particular SIM group must be in the same IP subnet (broadcast domain). Members of a SIM group cannot cross a router.

A SIM group accepts one Commander Switch (numbered 0) and up to 32 switches (numbered 0-31).

There is no limit to the number of SIM groups in the same IP subnet (broadcast domain), however a single switch can only belong to one group.

If multiple VLANs are configured, the SIM group will only utilize the default VLAN on any switch.

SIM allows intermediate devices that do not support SIM. This enables the user to manage a switch that are more than one hop away from the CS.

The SIM group is a group of switches that are managed as a single entity. The DGS-3700 Series may take on three different roles:

Commander Switch(CS) – This is a switch that has been manually configured as the controlling device for a group, and takes on the following characteristics:

- It has an IP Address.
- It is not a Commander Switch or Member Switch of another Single IP group.
- It is connected to the Member Switches through its management VLAN.

Member Switch(MS) – This is a switch that has joined a single IP group and is accessible from the CS, and it takes on the following characteristics:

- It is not a CS or MS of another IP group.
- It is connected to the CS through the CS management VLAN.

Candidate Switch(CaS) – This is a switch that is ready to join a SIM group but is not yet a member of the SIM group. The Candidate Switch may join the SIM group through an automatic function of the DGS-3700 Series, or by manually configuring it to be a MS of a SIM group. A switch configured as a CaS is not a member of a SIM group and will take on the following characteristics:

- It is not a CS or MS of another Single IP group.
- It is connected to the CS through the CS management VLAN.

The following rules also apply to the above roles:

1. Each device begins in the Commander state.
2. CS's must change their role to CaS and then to MS, to become a MS of a SIM group. Thus the CS cannot directly be converted to a MS.
3. The user can manually configure a CS to become a CaS.
4. A MS can become a CaS by:
   a. Being configured as a CaS through the CS.
   b. If report packets from the CS to the MS time out.
5. The user can manually configure a CaS to become a CS
6. The CaS can be configured through the CS to become a MS.

After configuring one switch to operate as the CS of a SIM group, additional DGS-3700 Series switches may join the group by either an automatic method or by manually configuring the Switch to be a MS. The CS will then serve as the in band entry point for access to the MS. The CS's IP address will become the path to all MS's of the group and the CS's Administrator's password, and/or authentication will control access to all MS's of the SIM group.

With SIM enabled, the applications in the CS will redirect the packet instead of executing the packets. The applications will decode the packet from the administrator, modify some data, then send it to the MS. After execution, the CS may receive a response packet from the MS, which it will encode and send back to the administrator.

When a CS becomes a MS, it automatically becomes a member of the first SNMP community (include read/write and read only) to which the CS belongs. However if a MS has its own IP address, it can belong to SNMP communities to which other switches in the group, including the CS, do not belong.

The Upgrade to v1.6

To better improve SIM management, the DGS-3700 Series has been upgraded to version 1.6 in this release. Many improvements have been made, including:

The Commander Switch (CS) now has the capability to automatically rediscover member switches that have left the SIM group, either through a reboot or web malfunction. This feature is accomplished through the use of Discover packets and Maintain packets that previously set SIM members will emit after a reboot. Once a MS has had its MAC address and password saved to the CS's database, if a reboot occurs in the MS, the CS will keep this MS information in its database and when a MS has been rediscovered, it will add the MS back into the SIM tree automatically. No configuration will be necessary to rediscover these switches. There are some instances where pre-saved MS switches cannot be rediscovered. For example, if the Switch is still powered down, if it has become the member of another group, or if it has been configured to be a Commander Switch, the rediscovery process cannot occur.

This version will support multiple switch upload and downloads for firmware, configuration files and log files, as follows:

- Firmware – The switch now supports multiple MS firmware downloads from a TFTP server.
- Configuration Files – This switch now supports multiple downloading and uploading of configuration files both to (for configuration restoration) and from (for configuration backup) MS's, using a TFTP server..
- Log – The switch now supports uploading multiple MS log files to a TFTP server.

NOTE: For more details regarding improvements made in SIMv1.6, please refer to the White Paper located on the D-Link website.

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

Command	Parameters
enable sim	
disable sim	
show sim	{[candidates { <candidate_id 1-100> } | members{ <member_id 1-32> } | group {commander_mac <macaddr>} | neighbor]}
reconfig	[member_id <value 1-32> | exit]
config sim_group	[add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]
config sim	[[commander { group_name <groupname 64>}|candidate]| dp_interval <sec 30-90> | hold_time <sec 100-255>]
download sim_ms	[firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}
upload sim_ms	[configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}

Each command is listed, in detail, in the following sections.

enable sim	
Purpose	Used to enable Single IP Management (SIM) on the Switch
Syntax	**enable sim**
Description	This command will enable SIM globally on the Switch. SIM features and functions will not function properly unless this function is enabled.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SIM on the Switch:

```
DGS-3700-12:5#enable sim
Command: enable sim

Success.

DGS-3700-12:5#
```

disable sim

Purpose	Used to disable Single IP Management (SIM) on the Switch
Syntax	**disable sim**
Description	This command will disable SIM globally on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable SIM on the Switch:

```
DGS-3700-12:5#disable sim
Command: disable sim

Success.

DGS-3700-12:5#
```

show sim

Purpose	Used to view the current information regarding the SIM group on the Switch.
Syntax	**show sim {[candidates { <candidate_id 1-100> } | members{ <member_id 1-32> } | group {commander_mac <macaddr>} | neighbor]}**
Description	This command will display the current information regarding the SIM group on the Switch, including the following: *SIM Version* – Displays the current Single IP Management version on the Switch. *Firmware Version* – Displays the current Firmware version on the Switch. *Device Name* – Displays the user-defined device name on the Switch. *MAC Address* – Displays the MAC Address of the Switch. Capabilities – Displays the type of switch, be it Layer 2 (L2) or Layer 3 (L3). *Platform* – Switch Description including name and model number. *SIM State* – Displays the current Single IP Management State of the Switch, whether it be enabled or disabled. *Role State* – Displays the current role the Switch is taking, including Commander, Member or Candidate. A Stand-alone switch will always have the commander role. *Discovery Interval* – Time in seconds the Switch will send discovery packets out over the network. *Hold time* – Displays the time in seconds the Switch will hold discovery results before dropping it or utilizing it.
Parameters	*candidates <candidate_id 1-100>* – Entering this parameter will display information concerning candidates of the SIM group. To view a specific candidate, include that candidate's ID number, listed from 1 to 100. *members <member_id 1-32>* – Entering this parameter will display information concerning members of the SIM group. To view a specific member, include that member's id number, listed from 1 to 32. *group {commander_mac <macaddr>}* – Entering this parameter will display information concerning the SIM group. To view a specific group, include the commander's MAC address of the group. *neighbor* – Entering this parameter will display neighboring devices of the Switch. A SIM neighbor is defined as a switch that is physically connected to the Switch but is not part of the SIM group. This screen will produce the following results: Port – Displays the physical port number of the commander switch where the uplink to the neighbor switch is located. MAC Address – Displays the MAC Address of the neighbor switch. Role – Displays the role(CS, CaS, MS) of the neighbor switch.
Restrictions	None.

Example usage:

To show the SIM information in detail:

```
DGS-3700-12:5#show sim
Command: show sim

SIM Version         : VER-1.61
Firmware Version    : 1.00.B035
Device Name         :
MAC Address         : 00-01-02-03-04-00
Capabilities        : L2
Platform            : DGS-3700-12 L2 Switch
SIM State           : Enabled
Role State          : Candidate
Discovery Interval : 30 sec
Hold Time           : 100 sec

DGS-3700-12:5#
```

To show the candidate information in summary, if the candidate ID is specified:

```
DGS-3700-12:5#show sim candidates
Command: show sim candidates

ID  MAC Address            Platform /             Hold      Firmware     Device Name
                           Capability             Time      Version
--- -----------------     ---------------------- -----     ---------   ------------
1   00-01-02-03-04-00      DGS-3700-12 L2 Switch   40        1.00.B035    The Man
2   00-55-55-00-55-00      DGS-3700-12 L2 Switch   140       1.00.B035    default

Total Entries: 2

DGS-3700-12:5#
```

To show the member information in summary:

```
DGS-3700-12:5#show sim members
Command: show sim members

ID    MAC Address         Platform /           Hold     Firmware      Device Name
                          Capability           Time     Version
--- --------------       --------------------- ------   ----------    -------------
1    00-01-02-03-04-00  DGS-3700-12 L2 Switch   40       1.00.B035     The Man
2    00-55-55-00-55-00  DGS-3700-12 L2 Switch   140      1.00.B035     default
master

Total Entries: 2

DGS-3700-12:5#
```

To show other groups information in summary, if group is specified:

```
DGS-3700-12:5#show sim group
Command: show sim group

SIM Group Name : default

ID  MAC Address           Platform /           Hold       Firmware     Device Name
                          Capability           Time       Version
--- ----------------  -------------------    -----     ----------    -------------
*1  00-01-02-03-04-00  DGS-3700-12 L2 Switch    40       1.00.B035    Trinity
 2  00-55-55-00-55-00  DGS-3700-12 L2 Switch   140       1.00.B035    default master

SIM Group Name : SIM2

ID  MAC Address           Platform /           Hold       Firmware    Device Name
                          Capability           Time       Version
---  ----------------   ------------------    ------     ---------   -------------
*1  00-01-02-03-04-00   DGS-3700-12 L2 Switch    40        1.00.B035  Neo
 2  00-55-55-00-55-00   DGS-3700-12 L2 Switch    140       1.00.B035  default master


DGS-3700-12:5#
```

Example usage:

To view SIM neighbors:

```
DGS-3700-12:5# show sim neighbor
Command: show sim neighbor

Neighbor Info Table

Port     MAC Address         Role
------   ------------------  ---------
1        00-35-26-00-11-99   Commander
1        00-35-26-00-11-91   Member
3        00-35-26-00-11-90   Candidate

Total Entries: 3

DGS-3700-12:5#
```

reconfig

Purpose	Used to connect to a member switch, through the commander switch, using Telnet.
Syntax	**reconfig [member_id <value 1-32> | exit]**
Description	This command is used to reconnect to a member switch using Telnet.
Parameters	*member_id <value 1-32>* – Select the ID number of the member switch to configure. *exit* – This command is used to exit from managing the member switch and will return to managing the commander switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To connect to the MS, with member ID 2, through the CS, using the command line interface:

```
DGS-3700-12:5#reconfig member_id 2
Command: reconfig member_id 2

DGS-3700-12:5#
Login:
```

config sim_group

Purpose	Used to add candidates and delete members from the SIM group.
Syntax	**config sim_group [add <candidate_id 1-100> {<password>} | delete <member_id 1-32>]**
Description	This command is used to add candidates and delete members from the SIM group by ID number.
Parameters	*add <candidate_id> <password>* – Use this parameter to change a candidate switch (CaS) to a member switch (MS) of a SIM group. The CaS may be defined by its ID number and a password (if necessary). *delete <member_id 1-32>* – Use this parameter to delete a member switch of a SIM group. The member switch should be defined by ID number.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add a member:

```
DGS-3700-12:5#config sim_group add 2
Command: config sim_group add 2

Please wait for ACK!!!
SIM Config Success !!!

Success.

DGS-3700-12:5#
```

To delete a member:

```
DGS-3700-12:5#config sim delete 1
Command: config sim delete 1

Please wait for ACK!!!
SIM Config Success!!!

DGS-3700-12:5#
```

config sim

Purpose	Used to configure role parameters for the SIM protocol on the Switch.
Syntax	**config sim [[commander { group_name <groupname 64>}|candidate]| dp_interval <sec 30-90> | hold_time <sec 100-255>]**
Description	This command is used to configure parameters of switches of the SIM.
Parameters	*commander* – Use this parameter to configure the commander switch (CS) for the following parameters: • *group_name <groupname 64>* – Used to update the name of the group. Enter an alphanumeric string of up to 64 characters to rename the SIM group. • *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from *30* to *90* seconds. • *hold time <sec 100-300>* – Using this parameter, the user may set the time, in seconds, the CS will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from *100* to *300* seconds. *candidate* – Used to change the role of a CS (commander) to a CaS (candidate). • *dp_interval <30-90>* – The user may set the discovery protocol interval, in seconds that the Switch will send out discovery packets. Returning information to the CS will include information about other switches connected to it. (Ex. MS, CaS). The user may set the *dp_interval* from *30* to *90* seconds. • *hold time <100-255>* – Using this parameter, the user may set the time, in seconds, the Switch will hold information sent to it from other switches, utilizing the discovery interval protocol. The user may set the hold time from *100* to *255* seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To change the time interval of the discovery protocol:

```
DGS-3700-12:5#config sim commander dp_interval 30
Command: config sim commander dp_interval 30

Success.

DGS-3700-12:5#
```

To change the hold time of the discovery protocol:

```
DGS-3700-12:5#config sim commander hold_time 120
Command: config sim commander hold_time 120

Success.

DGS-3700-12:5#
```

To transfer the CS (commander) to be a CaS (candidate):

```
DGS-3700-12:5#config sim candidate
Command: config sim candidate

Success.

DGS-3700-12:5#
```

To transfer the Switch to be a CS:

```
DGS-3700-12:5#config sim commander
Command: config sim commander

Success.

DGS-3700-12:5#
```

To update the name of a group:

```
DGS-3700-12:5#config sim commander group_name Trinity
Command: config sim commander group_name Trinity

Success.

DGS-3700-12:5#
```

download sim_ms

Purpose	Used to download firmware or configuration file to an indicated device.
Syntax	**download sim_ms [firmware_from_tftp | configuration_from_tftp] <ipaddr> <path_filename> {[members <mslist 1-32> | all]}**
Description	This command will download a firmware file or configuration file to a specified device from a TFTP server.
Parameters	*firmware_from_tftp* – Specify this parameter to download firmware to members of a SIM group. *configuration_from_tftp* – Specify this parameter to download a switch configuration to members of a SIM group. <*ipaddr*> – Enter the IP address of the TFTP server. <*path_filename*> – Enter the path and the filename of the firmware or switch on the TFTP server. *members* – Enter this parameter to specify the members to which the user prefers to download firmware or switch configuration files. The user may specify a member or members by adding one of the following: • <*mslist*> – Enter a value, or values to specify which members of the SIM group will receive the firmware or switch configuration. • *all* – Add this parameter to specify all members of the SIM group will receive the firmware or switch configuration.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download firmware:

```
DGS-3700-12:5#download sim_ms firmware_from_tftp 10.53.13.94 c:/des3526.had members
all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3526.had members all

This device is updating firmware. Please wait several minutes...

Download Status :

ID    MAC Address         Result
---  -----------------  ----------------
  1   00-01-02-03-04-00  Success
  2   00-07-06-05-04-03  Success
  3   00-07-06-05-04-03  Success

DGS-3700-12:5#
```

To download configuration files:

```
DGS-3700-12:5#download sim_ms configuration_from_tftp 10.53.13.94 c:/des3528.txt
members all
Command: download sim_ms firmware_from_tftp 10.53.13.94 c:/des3528.txt members all

This device is updating configuration. Please wait several minutes...

Download Status :

ID    MAC Address         Result
---  -----------------   ----------------
1     00-01-02-03-04-00   Success
2     00-07-06-05-04-03   Success
3     00-07-06-05-04-03   Success

DGS-3700-12:5#
```

upload sim_ms

Purpose	User to upload a configuration file to a TFTP server from a specified member of a SIM group.
Syntax	**upload sim_ms [configuration_to_tftp | log_to_tftp] <ipaddr> <path_filename> {[members <mslist> | all]}**
Description	This command will upload a configuration file to a TFTP server from a specified member of a SIM group.
Parameters	*configuration_from_tftp* – Specify this parameter to upload a switch configuration to members of a SIM group. *log_to_ftp* – Specify this parameter to upload a switch log to a member of the SIM group. *<ipaddr>* – Enter the IP address of the TFTP server to which to upload a configuration file. *<path_filename>* – Enter a user-defined path and file name on the TFTP server to which to upload configuration files. *members* – Enter this parameter to specify the members to which the user prefers to upload the switch configuration or log files. The user may specify a member or members by adding one of the following: • *<mslist>* – Enter a value, or values to specify which members of the SIM group will upload the switch configuration or log. *all* – Add this parameter to specify all members of the SIM group will upload the switch configuration or log.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To upload configuration files to a TFTP server:

```
DGS-3700-12:5# DGS-3700-12:5#upload sim_ms configuration_to_tftp 10.22.33.99
c:/configuration.txt members 1
Command: upload sim_ms configuration_to_tftp 10.22.33.99 c:/configuration.txt
members 1


Success.


DGS-3700-12:5#
```

22

DDM COMMANDS

The Digital Diagnostic Monitoring (DDM) module allows real time access to the SFP module operating parameters. The DDM commands allow users to set warning and alarm thresholds on the operating parameters. Once any of the operating parameters rise above the high threshold or fall below the low threshold, the abnormal or dangerous conditions will be logged or processed accordingly to user's configuration.

The following monitoring operating parameters can be accessed.

- Internally measure the transceiver temperature in degree Celsius.
- Internally measure the transceiver supply voltage in volts.
- Measures Tx bias current in mA.
- Measures Tx output power in mW.
- Measures Rx received optical power in mW.

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

Command	Parameters
config ddm temperature	config ddm ports [<portlist> | all] temperature_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} (1)
config ddm voltage	config ddm ports [<portlist> | all] voltage_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} (1)
config ddm bias current	config ddm ports [<portlist> | all] bias_current_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} (1)
config ddm tx power	config ddm ports [<portlist> | all] tx_power_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} (1)
config ddm rx power	config ddm ports [<portlist> | all] rx_power_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>} (1)
config ddm state	config ddm ports [<portlist> | all] state [enable | disable] (1)
config ddm shutdown	config ddm ports <portlist> | all] shutdown [alarm | warning | none] (1)
config ddm log	config ddm log [enable | disable]
config ddm trap	config ddm trap [enable | disable]
show ddm status	show ddm ports {<portlist>} status
show ddm config	show ddm ports {<portlist > } configuration
show ddm	show ddm

Each command is listed, in detail, in the following sections.

config ddm temperature

Purpose	To configure the thresholds of temperature for specified ports.
Syntax	**config ddm ports [<portlist> | all] temperature_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>}(1)**
Description	This command configures the temperature thresholds for specified ports.
Parameters	*all* – Indicates that all ports will be set. *<portlist>* – Specifies a port or range of ports to be set. *temperature_threshold* – Specifies the threshold of the SFP module's temperature. *high_alarm* – High threshold for alarm. When the operating parameter rises above this value, action associated with the alarm will be taken. *low_alarm* – Low threshold for alarm. When the operating parameter falls below this value, action associated with the alarm is taken. *high_warning* – High threshold for warning. When the operating parameter rises above this value, action associated with warning is taken. *low_warning* – Low threshold for warning. When the operating parameter falls below this value, action associated with this warning is taken.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's temperature threshold:

```
DGS-3700-12:5#config ddm ports 11 temperature_threshold high_alarm 85 low_alarm 15
high_warning 65 low_warning 20
Command: config ddm ports 11 temperature_threshold high_alarm 85 low_alarm 15
high_warning 65 low_warning 20

Success.

DGS-3700-12:5#
```

config ddm voltage

Purpose	This command configures the thresholds of voltage for the specified ports.
Syntax	**config ddm ports [<portlist> | all] voltage_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>}(1)**
Description	This command configures the voltage thresholds for specified ports.
Parameters	*all* – Indicates all ports will be set. *<portlist>* – Specifies a port or range of ports to be set. *voltage_threshold* – Specifies the threshold of the SFP module's voltage. *high_alarm* – High threshold for alarm. When the operating parameter rises above this value, action associated with the alarm is taken. *low_alarm* – Low threshold for alarm. When the operating parameter falls below this value, action associated with the alarm is taken. *high_warning* – High threshold for warning. When the operating parameter rises above this value, action associated with the warning is taken. *low_warning* – Low threshold for warning. When the operating parameter falls below this value, action associated with the warning is taken.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's voltage threshold:

```
DGS-3700-12:5#config ddm ports 11 voltage_threshold high_alarm 3.4 low_alarm 1 
high_warning 3.3 low_warning 1.5
Command: config ddm ports 11 voltage_threshold high_alarm 3.4 low_alarm 1 high_warning 
3.3 low_warning 1.5

Success.

DGS-3700-12:5#
```

config ddm bias current

Purpose	To configure the threshold of the bias current for specified ports.
Syntax	**config ddm ports [<portlist> | all] bias_current_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>}(1)**
Description	This command configures the bias current threshold for the specified ports.
Parameters	*all* – Indicates all ports will be set. *<portlist>* – Specifies a port or range of ports to be set. *bias_current_threshold* – Specifies the threshold of SFP module's bias current. *high_alarm* – High threshold for alarm. When the operating parameter rises above this value, action associated with the alarm is taken. *low_alarm* – Low threshold for alarm. When the operating parameter falls below this value, action associated with the alarm is taken. *high_warning* – High threshold for warning. When the operating parameter rises above this value, action associated with the warning is taken. *low_warning* – Low threshold for warning. When the operating parameter falls below this value, action associated with the warning is taken.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's bias current threshold:

```
DGS-3700-12:5#config ddm ports 11 bias_current_threshold high_alarm 120 low_alarm 10 
high_warning 110 low_warning 15
Command: config ddm ports 11 bias_current_threshold high_alarm 120 low_alarm 10 
high_warning 110 low_warning 15

Success.

DGS-3700-12:5#
```

config ddm tx power

Purpose	This command configures the threshold of tx power for specified ports.
Syntax	**config ddm ports [<portlist> | all] tx_power_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>}(1)**
Description	This command configures the threshold of tx power for specified ports.
Parameters	*all* – Indicates all ports will be set. *<portlist>* – Specifies a port or range of ports to be set. *tx_power_threshold* – Specifies the threshold of SFP module's tx power. *high_alarm* – High threshold for alarm. When the operating parameter rises above this value, action associated with the alarm is taken. *low_alarm* – Low threshold for alarm. When the operating parameter falls below this value, action associated with the alarm is taken. *high_warning* – High threshold for warning. When the operating parameter rises above this value, action associated with the warning is taken. *low_warning* – Low threshold for warning. When the operating parameter falls below this value, action associated with the warning is taken.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's tx power threshold:

```
DGS-3700-12:5#config ddm ports 11 tx_power_threshold high_alarm 6.5 low_alarm 1
high_warning 6 low_warning 1.5
Command: config ddm ports 11 tx_power_threshold high_alarm 6.5 low_alarm 1
high_warning 6 low_warning 1.5

Success.

DGS-3700-12:5#
```

config ddm rx power

Purpose	This command configures the threshold of rx power for specified ports.
Syntax	**config ddm ports [<portlist> | all] rx_power_threshold {high_alarm <float> | low_alarm <float> | high_warning <float> | low_warning <float>}(1)**
Description	This command configures the threshold of tx power for specified ports.
Parameters	*all* – Indicates all ports will be set. *<portlist>* – Specifies a port or range of ports to be set. *rx_power_threshold* – Specifies the threshold of SFP module's rx power. *high_alarm* – High threshold for alarm. When the operating parameter rises above this value, action associated with the alarm is taken. *low_alarm* – Low threshold for alarm. When the operating parameter falls below this value, action associated with the alarm is taken. *high_warning* – High threshold for warning. When the operating parameter rises above this value, action associated with the warning is taken. *low_warning* – Low threshold for warning. When the operating parameter falls below this value, action associated with the warning is taken.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's rx power threshold:

```
DGS-3700-12:5#config ddm ports 11 rx_power_threshold high_alarm 6.5 low_alarm 1
high_warning 6 low_warning 1.5
Command: config ddm ports 11 rx_power_threshold high_alarm 6.5 low_alarm 1
high_warning 6 low_warning 1.5

Success.

DGS-3700-12:5#
```

config ddm state

Purpose	This command configures the action when an exceeding alarm threshold event is encountered.
Syntax	**config ddm ports [<portlist> | all] state [enable |disable] (1)**
Description	This command configures the ddm state.
Parameters	*all* – Indicates all ports will be configured. *<portlist>* – Specifies a port or range of ports to be configured. *state* – Specifies the ddm state, if the ddm state was configured to disable, the action of log,trap,shudown will be ignored.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's ddm state:

```
DGS-3700-12:5#config ddm ports 11 state enable
Command: config ddm ports 11 state enable

Success.

DGS-3700-12:5#
```

config ddm shutdown

Purpose	To configure the shutdown mode that when the GBIC exceed, will shut down the port.
Syntax	**config ddm ports [<portlist> | all] shutdown [alarm | warning| none] (1)**
Description	This command is used to configure the shutdown action.
Parameters	*all* – Indicates all ports will be configured. *<portlist>* – Specifies a port or range of ports to be configured. *shutdown* – Specifies the shutdown of DDM features.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 11's shutdown action:

```
DGS-3700-12:5#config ddm ports 11 shutdown alarm
Command: config ddm ports 11 shutdown alarm

Success.

DGS-3700-12:5#
```

config ddm log

Purpose	To configure the global log state.
Syntax	**config ddm log [enable|disable]**
Description	This command is used to configure the log state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure log state:

```
DGS-3700-12:5#config ddm log enable
Command: config ddm log enable

Success.

DGS-3700-12:5#
```

config ddm trap

Purpose	To configure the global trap state.
Syntax	**config ddm trap [enable|disable]**
Description	This command is used to configure the trap state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure trap state:

```
DGS-3700-12:5#config ddm trap enable
Command: config ddm trap enable

Success.

DGS-3700-12:5#
```

show ddm status

Purpose	Used to display the current operating ddm parameter values of the SFP module for the specified ports.
Syntax	**show ddm ports {<portlist>} status**
Description	This command is used to display the current operating parameters of the SFP modules.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display port 10-12's operating parameters:

```
DGS-3700-12:5#show ddm ports 10-12 status
Command:show ddm ports 10-12 status

 Port    Temperature   Voltage    Bias Current   TX Power     RX Power
        (in Celsius)     (V)         (mA)         (mW)         (mW)
------- ------------ ---------- ------------- ---------- ------------
  10         -            -           -            -            -
  11         -            -           -            -            -
  12         -            -           -            -            -

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

show ddm config

Purpose	Used to display the current configurations of the digital diagnostics monitoring function.
Syntax	**show ddm ports {<portlist>} configuration**
Description	This command is used to display the current configurations of the digital diagnostics monitoring function.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display port 11's configuration:

```
DGS-3700-12:5#show ddm ports 11 configuration
Command: show ddm ports 11 configuration

Port:            11
-----------------------------------------
DDM state : Enabled
Shutdown  : Alarm

Threshold       Temperature    Voltage   Bias-Current   TX-Power  RX-Power
               (in Celsius)      (V)        (mA)         (mW)      (mW)

------------ -------------- ---------- ------------- ---------- ------
High Alarm        85(A)         3.4          120          6.5       6.5
Low Alarm         15            1            10           1(A)       1
High Warning      65            3.3          110(A)       6         6
Low Warning       20            1.5(A)       15           1.5       1.5

A means that the threshold is administratively configured.

DGS-3700-12:5#
```

Show ddm

Purpose	To show the ddm global configuration
Syntax	**show ddm**
Description	This command is used to show ddm global configuration
Parameters	None.
Restrictions	None.

Example usage:

To show ddm global configuration :

```
DGS-3700-12:5#show ddm
Command: show ddm

DDM Log           :Disabled
DDM Trap          :Disabled

Success.

DGS-3700-12:5#
```

23

VLAN COMMANDS

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

Command	Parameters
create vlan	< vlan_name 32> tag <vlanid 2-4094> {type 1q_vlan advertisement}
create vlan vlanid	<vidlist> { advertisement }
delete vlan	<vlan_name 32>
delete vlan vlanid	<vidlist>
config vlan	<vlan_name 32> {[add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)
config vlan vlanid	<vidlist> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]| name <vlan_name 32>}(1)
config port_vlan	[<portlist> | all] { gvrp_state [enable | disable]|ingress_checking [enable | disable] |acceptable_frame[tagged_only | admit_all] | pvid<vlanid 1-4094>}(1)
enable gvrp	
disable gvrp	
show vlan	<vlan_name 32> | vlanid < vidlist > | ports <portlist>
show port_vlan	<portlist>
create dot1v_protocol_group	group_id <id 1-16> {group_name <name 32>}
config dot1v_protocol_group	[group_id < id 1-16> | group_name <name 32>] add protocol [ethernet_2| ieee802.3_snap| ieee802.3_llc] < protocol_value>
config dot1v_protocol_group	[group_id < id 1-16> | group_name <name 32>] delete protocol [ethernet_2 | ieee802.3_snap | ieee802.3_llc] < protocol_value>
delete dot1v_protocol_group	[group_id <id 1-16> | group_name <name 32>| all]
show dot1v_protocol_group	{group_id <id 1-16> | group_name <name 32>}
config port dot1v ports	[<portlist> | all] [add protocol_group [group_id <id 1-16> | group_name <name 32>] [vlan< vlan_name 32> | vlanid <id>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-16>|all]]
show port dot1v	{ports <portlist>}
enable pvid auto_assign	
disable pvid auto_assign	
show pvid auto_assign	
config gvrp	[timer [join | leave | leaveall] < value 100-100000> | nni_bpdu_addr [dot1d | dot1ad]]
show gvrp	

Each command is listed, in detail, in the following sections.

create vlan

Purpose	Used to create a VLAN on the Switch.
Syntax	**create vlan <vlan_name 32 > tag <vlanid 2-4094> { type 1q_vlan advertisement }**
Description	This command allows the user to create a VLAN on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN to be created. *<vlanid 2-4094>* – The VLAN ID of the VLAN to be created. Allowed values = 2-4094 *advertisement* – Specifies that the VLAN is able to join GVRP.
Restrictions	Each VLAN name can be up to 32 characters. Up to 4094 static VLANs may be created per configuration. Only Administrator and Operator-level users can issue this command.

Example usage:

To create a VLAN v1, tag 2:

```
DGS-3700-12:5#create vlan v1 tag 2
Command: create vlan v1 tag 2

Success.

DGS-3700-12:5#
```

create vlan vlanid

Purpose	Used to create multiple VLANs by VLAN ID list on the switch.
Syntax	**create vlan vlanid <vidlist> { advertisement }**
Description	This command is used to create multiple VLANs on the switch.
Parameters	*<vidlist>* – Specifies a range of multiple VLAN IDs to be created. *advertisement* – Join GVRP or not. If not, the VLAN can't join dynamically.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a VLAN ID on the Switch:

```
DGS-3700:5#create vlan vlanid 5 advertisement
Command: create vlan vlanid 5 advertisement

Success

DGS-3700:5#
```

delete vlan

Purpose	Used to delete a previously configured VLAN on the Switch.
Syntax	**delete vlan <vlan_name 32>**
Description	This command is used to delete a previously configured VLAN on the Switch.
Parameters	*<vlan_name 32>* – The VLAN name of the VLAN to delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To remove the VLAN "v1":

```
DGS-3700-12:5#delete vlan v1
Command: delete vlan v1

Success.

DGS-3700-12:5#
```

delete vlan vlanid

Purpose	Used to delete multiple VLANs by VLAN ID on the switch.
Syntax	**delete vlan vlanid <vidlist>**
Description	This command is used to delete previously configured multiple VLANs on the switch.
Parameters	*<vidlist>* – Specifies a range of multiple VLAN IDs to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete VLAN ID on the switch:

```
DGS-3700-12:5#delete vlan vlanid 5
Command: delete vlan vlanid 5

Success

DGS-3700-12:5#
```

config vlan

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan <vlan_name 32> { [add [tagged | untagged | forbidden] | delete] <portlist> | advertisement [enable | disable]}(1)**
Description	This command allows the user to add ports to the port list of a previously configured VLAN. The user can specify the additional ports as tagging, untagging, or forbidden. The default is to assign the ports as untagging.
Parameters	*<vlan_name 32>* – The name of the VLAN to which to add ports. *add* – Entering the add parameter will add ports to the VLAN. There are three types of ports to add: • *tagged* – Specifies the additional ports as tagged. • *untagged* – Specifies the additional ports as untagged. • *forbidden* – Specifies the additional ports as forbidden. *delete* – Deletes ports from the specified VLAN. *<portlist>* – A port or range of ports to add to, or delete from the specified VLAN. *advertisement [enable | disable]* – Enables or disables GVRP on the specified VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add 4 through 8 as tagged ports to the VLAN v1:

```
DGS-3700-12:5#config vlan v1 add tagged 4-8
Command: config vlan v1 add tagged 4-8

Success.

DGS-3700-12:5#
```

To delete ports from a VLAN:

```
DGS-3700-12:5#config vlan v1 delete 6-8
Command: config vlan v1 delete 6-8

Success.

DGS-3700-12:5#
```

config vlan vlanid

Purpose	Used to add additional ports to a previously configured VLAN.
Syntax	**config vlan vlanid <vidlist> {add [tagged | untagged | forbidden] | delete <portlist> | advertisement [enable | disable] | name <vlan_name 32>}(1)**
Description	This command allows you to add or delete ports of the port list of previously configured VLAN(s). You can specify the additional ports as being tagged, untagged or forbidden. The same port is allowed to be an untagged member port of multiple VLAN's. You can also specify if the ports will join GVRP or not with the *advertisement* parameter. The *name* parameter allows you to specify the name of the VLAN that needs to be modified.
Parameters	*<vidlist>* – Specifies a range of multiple VLAN IDs to be configured. *tagged* – Specifies the additional ports as tagged. *untagged* – Specifies the additional ports as untagged. *forbidden* – Specifies the additional ports as forbidden. *<portlist>* – A range of ports to add to the VLAN. *advertisement* – Entering the advertisement parameter specifies if the port should join GVRP or not. There are two parameters: ▪ *enable* – Specifies that the port should join GVRP. ▪ *Disable* – Specifies that the port should not join GVRP. *name* – Entering the name parameter specifies the name of the VLAN to be modified. <*name*> – Enter a name for the VLAN
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config vlan vlanid on the switch:

```
DGS-3700-12:5#config vlan vlanid 5 add tagged 7 advertisement enable name RG
Command: config vlan vlanid 5 add tagged 7 advertisement enable name RG

Success.

DGS-3700-12:5#
```

config port_vlan

Purpose	Used to configure GVRP on the Switch.
Syntax	**config port_vlan [<portlist> | all] { gvrp_state [enable | disable]|ingress_checking [enable | disable] |acceptable_frame[tagged_only | admit_all]pvid<vlanid 1-4094>}(1)**
Description	This command is used to configure the Group VLAN Registration Protocol on the Switch. Ingress checking, the sending and receiving of GVRP information, and the Port VLAN ID (PVID) can be configured.
Parameters	*<portlist>* – A port or range of ports for which users want to enable GVRP for. *all* – Specifies all of the ports on the Switch. *state [enable* | *disable]* – Enables or disables GVRP for the ports specified in the port list. *ingress_checking [enable* | *disable]* – Enables or disables ingress checking for the specified port list. *acceptable_frame [tagged_only* | *admit_all]* – This parameter states the frame type that will be accepted by the Switch for this function. *tagged_only* implies that only VLAN tagged frames will be accepted, while *admit_all* implies tagged and untagged frames will be accepted by the Switch. *pvid <vlanid 1-4094>* – Specifies the default VLAN associated with the port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the ingress checking status, the sending and receiving GVRP information:

```
DGS-3700-12:5#config port_vlan 1-4 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2
Command: config port_vlan 1-4 gvrp_state enable ingress_checking enable
acceptable_frame tagged_only pvid 2

Success.

DGS-3700-12:5#
```

enable gvrp

Purpose	Used to enable the Generic VLAN Registration Protocol (GVRP).
Syntax	**enable gvrp**
Description	This command, along with **disable gvrp** below, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the generic VLAN Registration Protocol (GVRP):

```
DGS-3700-12:5#enable gvrp
Command: enable gvrp

Success.

DGS-3700-12:5#
```

disable gvrp

Purpose	Used to disable the Generic VLAN Registration Protocol (GVRP).
Syntax	**disable gvrp**
Description	This command, along with **enable gvrp**, is used to enable and disable GVRP on the Switch, without changing the GVRP configuration on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the Generic VLAN Registration Protocol (GVRP):

```
DGS-3700-12:5#disable gvrp
Command: disable gvrp

Success.

DGS-3700-12:5#
```

show vlan

Purpose	Used to display the current VLAN configuration on the Switch
Syntax	**show vlan { <vlan_name 32> | vlanid <vidlist> | ports <portlist>}**
Description	This command displays summary information about each VLAN including the VLAN ID, VLAN name, the Tagging/Untagging status, and the Member/Non-member/Forbidden status of each port that is a member of the VLAN.
Parameters	*<vlan_name 32>* – The VLAN name of the VLAN for which to display a summary of settings.
Restrictions	None.

Example usage:

To display the Switch's current VLAN settings:

```
DGS-3700-12:5#show vlan
Command: show vlan

VID             : 1          VLAN Name     : default
VLAN Type       : Static     Advertisement : Enabled
Member Ports    : 1-12
Static Ports    : 1-12
Current Tagged Ports  :
Current Untagged Ports: 1-12
Static Tagged Ports   :
Static Untagged Ports : 1-12
Forbidden Ports       :

VID             : 2          VLAN Name     : v1
VLAN Type       : Static     Advertisement : Disabled
Member Ports    :
Static Ports    :
Current Tagged Ports  :
Current Untagged Ports:
Static Tagged Ports   :
Static Untagged Ports :
Forbidden Ports       :

 Total Entries: 2
DGS-3700-12:5#
```

```
DGS-3700-12:5# show vlan ports 1-4
Command: show vlan ports 1-4

Port    VID   Untagged  Tagged  Dynamic  Forbidden
-----   ----  --------  ------  -------  ---------
 1      1       X         -       -        -
 2      1       X         -       -        -
 3      1       X         -       -        -
 4      1       X         -       -        -

DGS-3700-12:5#
```

show port_vlan

Purpose	Used to display the GVRP status for a port list on the Switch.
Syntax	**show port_vlan <portlist>**
Description	This command displays the GVRP status for a port list on the Switch
Parameters	*<portlist>* – Specifies a port or range of ports for which the GVRP status is to be displayed.
Restrictions	None.

Example usage:

To display GVRP port status:

```
DGS-3700-12:5#show port_vlan 1-10
Command: show port_vlan 1-10

Global GVRP : Disabled

Port      PVID       GVRP           Ingress Checking     Acceptable Frame Type
------    ----       --------       ---------------      ---------------------
1           1        Disabled       Enabled               All Frames
2           1        Disabled       Enabled               All Frames
3           1        Disabled       Enabled               All Frames
4           1        Disabled       Enabled               All Frames
5           1        Disabled       Enabled               All Frames
6           1        Disabled       Enabled               All Frames
7           1        Disabled       Enabled               All Frames
8           1        Disabled       Enabled               All Frames
9           1        Disabled       Enabled               All Frames
10          1        Disabled       Enabled               All Frames

Total Entries : 10
```

create dot1v_protocol_group

Purpose	Create a protocol group for protocol VLAN function.
Syntax	**create dot1v_protocol_group group_id <id 1-16> {group_name <name 32>}**
Description	This command is used to create a protocol group for protocol VLAN function.
Parameters	*group_id* – The id of a protocol group which is used to identify a set of protocols. *group_name* – The name of the protocol group. The maximum length is 32 characters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a protocol group:

```
DGS-3700-12:5#create dot1v_protocol_group group_id 1 group_name General_Group
Command: create dot1v_protocol_group group_id 1 group_name General_Group

Success.

DGS-3700-12:5#
```

config dot1v_protocol_group add protocol

Purpose	Add a protocol to a protocol group.
Syntax	**config dot1v_protocol_group [group_id <id 1-16>| group_name <name>] add protocol [ethernet_2| ieee802.3_snap|ieee802.3_llc] < protocol_value>**
Description	This command adds a protocol to a protocol group.The selection of a protocol can be a pre-defined protocol type or a user defined protocol.
Parameters	*group_id* – The id of protocol group which is used to identify a set of protocols. *group_name* – The name of the protocol group. The maximum length is 32 characters. *protocol_value* – The protoocl vlaue is used to identify a protocol of the frame type specified. Depending on the frame type, the octet string will have one of the following values: The form of the input is 0x0 to 0xffff. For 'ethernet'II, this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,.. and so on. For ' IEEE802.3 SNAP ',this is this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,. and so on. For 'IEEE802.3 LLC', this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet is for Destination Service Access Point (DSAP), and second octet is for Source.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a protocol IPv6 to protocol group 1:

```
DGS-3700-12:5#config dot1v_protocol_group group_id 1 add protocol  ethernet_2  86DD
Command: config dot1v_protocol_group group_id 1 add protocol  ethernet_2  86DD

Success.

DGS-3700-12:5#
```

config dot1v_protocol_group delete protocol

Purpose	Used to delete a protocol from protocol group.
Syntax	**config dot1v_protocol_group [group_id < id>| group_name <name>] delete protocol [ethernet_2| ieee802.3_snap|** **ieee802.3_llc] < protocol_value.>**
Description	This command is used to delete a protocol from a protocol group.
Parameters	*group_id* – The id of protocol group which is used to identify a set of protocols. *group_name* – The name of the protocol group. The maximum length is 32 characters. *protocol_value* – The protoocl vlaue is used to identify a protocol of the frame type specified. Depending on the frame type, the octet string will have one of the following values: The form of the input is 0x0 to 0xffff. For 'ethernet'II, this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,. and so on. For ' IEEE802.3 SNAP ',this is this is a 16-bit (2-octet) hex value. Example: Ipv4 is 800, ipv6 is 86dd, ARP is 806,. and so on. For 'IEEE802.3 LLC', this is the 2-octet IEEE 802.2 Link Service Access Point (LSAP) pair: first octet is for Destination Service Access Point (DSAP), and second octet is for Source.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete protocol ipv6 from a protocol group 1:

```
DGS-3700-12:5#config dot1v_protocol_group group_id 1 delete protocol  ethernet_2  86DD
Command: config dot1v_protocol_group group_id 1 delete protocol  ethernet_2  86DD

Success.

DGS-3700-12:5#
```

delete dot1v_protocol_group

Purpose	Delete a protocol group.
Syntax	**delete dot1v_protocol_group [group_id <id 1-16>| group_name <name 32>| all]**
Description	This command deletes a protocol group.
Parameters	*group_id* – The id of protocol group which is used to identify a set of protocols. *group_name* – The name of the protocol group. The maximum length is 32 characters.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete protocol group 1:

```
DGS-3700-12:5#delete dot1v_protocol_group group_id 1
Command: delete dot1v_protocol_group group_id 1

Success.

DGS-3700-12:5#
```

show dot1v_protocol_group

Purpose	Display the protocols defined in a protocol group.
Syntax	**show dot1v_protocol_group {group_id <id 1-16> | group_name <name 32>}**
Description	This command is used to display the protocols defined in protocol groups.
Parameters	*group_id* – The id of protocol group which is used to identify a set of protocols. *group_name* – The name of the protocol group. The maximum length is 32 characters.
Restrictions	None.

Example usage:

To display the protocol group ID 1:

```
DGS-3700-12:5#show dot1v_protocol_group group_id 1
Command: show dot1v_protocol_group group_id 1

Protocol Group ID    Protocol Group Name    Frame Type     Protocol Value
-----------------    --------------------   -----------    --------------
1                    General Group          EthernetII        86DD

Total Entries: 1
DGS-3700-12:5#
```

config port dot1v

Purpose	Assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured.
Syntax	**config port dot1v ports [<portlist> | all] [add protocol_group [group_id <id>| group_name <name 32>] [vlan < vlan_name 32> | vlanid <id 1-16>] {priority <value 0-7>} | delete protocol_group [group_id <id 1-16>|all]]**
Description	This command is used to assign the VLAN for untagged packets ingress from the portlist based on the protocol group configured. This assignment can be removed by using delete protocol_group option. When priority is not specified in the command, the port default prority will be the priority for those untagged packets classified by the protocol vlan.
Parameters	*<portlist>* – Specifies a range of ports to apply this command. *group_id* – The id of protocol group which is used to identify a set of protocols. *group_name* – The name of the protocol group. The maximum length is 32 characters. *vlan* – Vlan that is to be associated with this protocol group on this port. *vlan_id* – Specifies the VLAN id. priority – Specifies the priority to be associated with the packet which has been classified to the specified vlan by the protocol.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

The example is to assign VLAN marketing-1 for untaged IPv6 packet ingress from port 3

To configure the group ID 1 on port 3 to be associated with VLAN marketing-1:

```
DGS-3700-12:5#config port dot1v ports 3 add protocol_group group_id 1 vlan marketing_1
Command: config port dot1v ports 3 add protocol_group group_id 1 vlan marketing_1

Success.

DGS-3700-12:5#
```

show port dot1v

Purpose	Display the VLAN to be associated with untagged packet ingressed from a port based on the protocol group.
Syntax	**show port dot1v{ ports <portlist>}**
Description	This command is used to display the VLAN to be associated with untagged packet ingressed from a port based on the protocol group.
Parameters	*portlist* – Specifies a range of ports to apply this command.
Restrictions	None.

Example usage:

The example display the protocol VLAN information for ports 1-2:

```
DGS-3700-12:5#show port dot1v ports 1-2
Command: show port dot1v ports 1-2


Port : 1
Protocol Group ID     VLAN Name          Protocol Priority
-----------------     ----------------   -----------------
1                      default                  -
2                      vlan_2                   -
3                      vlan_3                   -
4                      vlan_4                   -

Port : 2
Protocol Group ID     VLAN Name          Protocol Priority
-----------------     ------------       -----------------
1                       vlan_2                 -
2                       vlan_3                 -
3                       vlan_4                 -
4                       vlan_5                 -

Total Entries: 2
DGS-3700-12:5#
```

enable pvid auto_assign

Purpose	Enable/disable auto assignment of pvid.
Syntax	**enable|disable pvid auto_assign**
Description	The command enables the auto-assign of PVID. If "auto-assign PVID" is disabled, PVID only be changed by PVID configuration (user changes explicitly). The VLAN configuration will not automatically change PVID. If "Auto-assign PVID" is enabled, PVID will be possibly changed by PVID or VLAN configuration. When user configures a port to VLAN *X*'s untagged membership, this port's PVID will be updated with VLAN X. In the form of VLAN list command, PVID is updated with last item of VLAN list. When user removes a port from the untagged membership of the PVID's VLAN, the port's PVID will be assigned with "default VLAN". The default setting is enabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the auto-assign PVID:

```
DGS-3700-12:5#enable pvid auto_assign
Command: enable pvid auto_assign

Success.

DGS-3700-12:5#
```

show pvid auto_assign

Purpose	Show PVID auto-assigment state.
Syntax	**show pvid auto_assign**
Description	This command is used to display PVID auto-assignment state.
Parameters	None.
Restrictions	None.

Example usage:

To display PVID auto-assignment state:

```
DGS-3700-12:5#show pvid auto_assign
Command: show pvid auto_assign

PVID Auto-assignment: Enabled

DGS-3700-12:5#
```

config gvrp timer

Purpose	Used to configure the timer's value of GVRP and MAC address of GVRP's PDU of NNI port in Q-in-Q mode.
Syntax	**config gvrp [timer [join | leave | leaveall] < value 100-100000> | nni_bpdu_addr [dot1d | dot1ad]]**
Description	This command is used to set the GVRP timer's value and GVRP's PDU MAC address of NNI port in Q-in-Q mode. The default value for Join time is *200* milliseconds; for Leave time is *600* milliseconds; for LeaveAll time is *10000* milliseconds. The GVRP's PDU MAC address can be set to which is defined in 802.1d or 802.1ad.
Parameters	*timer* – Specifies GVRP timer will be set. *join* – Specifies the Join time will be set *leave* – Specifies the Leave time will be set *leaveall* – Specifies the LeaveAll time will be set *value* – The time value will be set. The value range is *100* to *100000* milliseconds. In addition, the Leave time should greater than 2 Join times and the LeaveAll time should greater than Leave time. *nni_bpdu_addr* – Specifies GVRP's PDU MAC address of NNI port in Q-in-Q mode will be set. *dot1d* – Specifies GVRP's PDU MAC address of NNI port using 802.1d's definement. *dot1ad* – Specifies GVRP's PDU MAC address of NNI port using 802.1ad's definement.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the Join time to 200 milliseconds:

```
DGS-3700-12:5#config gvrp timer join 200
Command: config gvrp timer join 200

Success.

DGS-3700-12:5#
```

show gvrp

Purpose	Used to display the timer's value and NNI BPDU address of GVRP.
Syntax	**show gvrp**
Description	This command is used to display the timer's value of GVRP.
Parameters	None.
Restrictions	None.

Example usage:

To display the timer's value of GVRP:

```
DGS-3700-12:5#show gvrp
Command: show gvrp

 Join Time:     200 Milliseconds
 Leave Time:    600 Milliseconds
 LeaveAll Time: 10000 Milliseconds
 NNI BPDU Address: dot1ad

DGS-3700-12:5#
```

24

STATIC SUBNET VLAN COMMANDS

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

Command	Parameters
create subnet_vlan	[network <network_address> |ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> |vlanid <vlanid 1-4094>] {priority <value 0-7>}
delete subnet_vlan	[network <network_address> | ipv6network <ipv6networkaddr>] | vlan <vlan_name 32> | vlanid <vidlist>| all]
show subnet_vlan	{[network<network_address> | ipv6network<ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist>]}
config vlan_precedence	ports <portlist> [mac_based_vlan | subnet_vlan]
show vlan_precedence	ports {<portlist>}

Each command is listed, in detail, in the following sections.

create subnet_vlan

Purpose	Used to create a static subnet VLAN entry.
Syntax	**create subnet_vlan [network <network_address> |ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> |vlanid <vlanid 1-4094>] {priority <value 0-7>}**
Description	This command is used to create a subnet VLAN entry. A subnet VLAN entry is an IP subnet-based VLAN classification rule. If an untagged or priority-tagged IP packet is received on a port, its source IP address will be used to match the subnet VLAN entries. If the source IP is in the subnet of an entry, the packet will be classified to the VLAN defined for this subnet.
Parameters	*network* – Is used to specify an IPv4 network address. The format is ipaddress/prefix length. *ipv6network* – Is used to specify an IPv6 network address. The format is ipaddress/prefix length. The prefix length of the IPv6 network address cannot be greater than 64. *vlan* – The VLAN to be associated with the subnet. You can specify a VLAN name or VLAN ID. The VLAN must be an existing static VLAN. *priority* – The priority to be associated with the subnet. Its range is 0-7.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create subnet VLAN:

```
DGS-3700-12:5#create subnet_vlan network 172.168.1.1/24 vlan v3 priority 2
Command: create subnet_vlan network 172.168.1.1/24 vlan v3 priority 2

Success.

DGS-3700-12:5#
```

delete subnet_vlan

Purpose	Used to delete a static subnet VLAN entry.
Syntax	**delete subnet_vlan [network <network_address> |ipv6network <ipv6networkaddr>] [vlan <vlan_name 32> |vlanid <vlanid 1-4094>] {priority <value 0-7>}**
Description	This command is used to delete a subnet VLAN entry. Subnet VLAN entries can be deleted by IP subnet or VLAN, or delete all subnet VLAN entries.
Parameters	*network* – To specify an IPv4 network address. The format is ipaddress/prefix length. *ipv6network* – To specify an IPv6 network address. The format is ipaddress/prefix length.The prefix length of IPv6 network address shall not be greater than 64. *vlan* – The VLAN to be associated with the subnet. You can specify a VLAN name or VLAN ID. *all* – All subnet VLAN entries will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete subnet VLAN:

```
DGS-3700-12:5#delete subnet_vlan network 172.168.1.1/24
Command: delete subnet_vlan network 172.168.1.1/24

Success.

DGS-3700-12:5#
```

show subnet_vlan

Purpose	This command is used to show static subnet VLAN entries.
Syntax	**show subnet_vlan {[network<network_address> | ipv6network<ipv6networkaddr> | vlan <vlan_name 32> | vlanid <vidlist>]}**
Description	This command is used to display subnet VLAN entries.
Parameters	*network* – To specify an IPv4 network address. The format is ipaddress/prefix length. *ipv6network* – To specify an IPv6 network address. The format is ipaddress/prefix length.The prefix length of IPv6 network address can not be greater than 64. *vlan* – The VLAN to be associated with the subnet. You can specify a VLAN name or VLAN ID.
Restrictions	None.

Example usage:

To display subnet VLAN:

```
DGS-3700-12:5#show subnet_vlan network 172.168.1.1/24
Command: show subnet_vlan network 172.168.1.1/24

IP Address/Subnet mask                          VLAN        Priority
----------------------------------------     -------     ---------
172.168.1.0/255.255.255.0                      3           2

DGS-3700-12:5#
```

config vlan_precedence ports

Purpose	Used to configure the VLAN classification precedence.
Syntax	**config vlan_precedence ports <portlist> [mac_based_vlan | subnet_vlan]**
Description	This command is used to configure VLAN classification precedence on each port. You can specify the order of MAC-based VLAN classifications and subnet VLAN classifications. If a port's VLAN classificataion is a MAC-based precedence, MAC-based VLAN classification will process first. If MAC-based VLAN classification fails, the subnet VLAN classification will be executed. If a port's VLAN classification is subnet VLAN precedence, the subnet VLAN classification will process first. If subnet VLAN classification fails, the MAC-based VLAN classification will be executed.
Parameters	*portlist* – To specify a range of ports *mac_based_vlan* – If the parameter is specified, the MAC-based VLAN classification is given precedence over the subnet VLAN classification *subnet_vlan* – If the parameter is specified, the subnet VLAN classification is given precedence over the MAC-based VLAN classification.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure VLAN precedence:

```
DGS-3700-12:5#config vlan_precedence ports 1 subnet_vlan
Command: config vlan_precedence ports 1 subnet_vlan

Success.

DGS-3700-12:5#
```

show vlan_precedence ports

Purpose	Used to show the VLAN classification precedence.
Syntax	**show vlan_precedence ports {<portlist>}**
Description	This command is used to show VLAN classification precedence on each port.
Parameters	*portlist* – To specify a range of ports. If not specified, all ports will be displayed.
Restrictions	None

Example usage:

To display VLAN precedence:

```
DGS-3700-12:5#show vlan_precedence ports 1-5
Command: show vlan_precedence ports 1-5

Port       VLAN Precedence
----       -----------------
1          Subnet VLAN
2          MAC-Based VLAN
3          MAC-Based VLAN
4          MAC-Based VLAN
5          MAC-Based VLAN

DGS-3700-12:5#
```

25

Q-IN-Q COMMANDS

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

Command	Parameters
enable qinq	
disable qinq	
show qinq	
config qinq ports	[<portlist>|all] {role [uni | nni] | missdrop [enable | disable]| tpid <hex 0x1 - 0xffff>| use_inner_priority [enable|disable]| vlan_preservation [enable | disable]| add_inner_tag [<hex 0x1 - 0xffff> |disable]}(1)
show qinq ports	{<portlist>}
create vlan_translation ports	[<portlist> | all] cvid <vidlist> [add| replace] svid <vlanid 1-4094> {priority <value 0-7>}
delete vlan_translation ports	[<portlist> | all] {cvid <vidlist>}
show vlan_translation	{ports <portlist> }

Each command is listed, in detail, in the following sections.

enable qinq

Purpose	Used to enable Q-in-Q mode.
Syntax	**enable qinq**
Description	This command enables Q-in-Q mode. When enable Q-in-Q, all network port roles will be NNI port and their outer TPID will be set to 88A8. All existed static VLAN will run as SP-VLAN. All dynamically learned L2 address will be cleared. All dynamically registered VLAN entries will be cleared, GVRP will be disabled. If you need to run GVRP on the switch, you shall enable GVRP manually. In Q-in-Q mode, SP-VLAN GVRP Address (01-80-C2-00-00-0D) or C-VLAN GVRP Address (01-80-C2-00-00-21) will be used by GVRP protocol. The default setting of Q-in-Q is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable Q-in-Q:

```
DGS-3700-12:5#enable qinq
Command: enable qinq

Success.

DGS-3700-12:5#
```

disable qinq

Purpose	Used to disable the Q-in-Q mode.
Syntax	**disable qinq**
Description	This 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. GVRP will be disabled. If you need to run GVRP on the switch, you shall enable GVRP manually. All existed SP-VLAN will run as static 1Q VLAN.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable Q-in-Q:

```
DGS-3700-12:5#disable qinq
Command: disable qinq

Success.

DGS-3700-12:5#
```

show qinq

Purpose	Used to show global Q-in-Q.
Syntax	**show qinq**
Description	This command is used to show the global Q-in-Q status.
Parameters	None.
Restrictions	None.

Example usage:

To show global Q-in-Q status:

```
DGS-3700-12:5#show qinq
Commands: show qinq

 QinQ Status: Enabled

DGS-3700-12:5#
```

configure qinq ports

Purpose	Used to configure Q-in-Q port.
Syntax	**config qinq ports [<portlist>|all] {role [uni | nni] | missdrop [enable | disable]| tpid <hex 0x1 - 0xffff>| use_inner_priority [enable|disable]| vlan_preservation [enable | disable]| add_inner_tag [<hex 0x1 - 0xffff> |disable]}(1)**
Description	This command is used to configure the Q-in-Q VLAN mode for ports, include: port role in double tag VLAN mode, enable/disable SP-VLAN assignment miss drop, and port outer TPID. If missdrop is enabled, the packet that does not match any assignment rule in the Q-in-Q profile will be dropped. If disabled, then the packet will be assigned to the PVID of the received port. This setting will not be effective when Q-in-Q mode is disabled.
Parameters	*portlist* – A range of ports to configure. *role* – Port role in Q-in-Q mode, it can be either UNI port or NNI port. UNI – User-to-Network Interface specifies that communication between the specified user and a specified network will occur. NNI – Network-to-Network Interface speficies that communication between two specified networks will occur. *missdrop* – enable/disable C-VLAN based SP-VLAN assignment miss drop. *outer_tpid* – Allows the interoperation with devices on a public network by specifying ports. *use_inner_priority* – Specify whether to use the priority in the C-VLAN tag as the priority in the SP-VLAN tag. *add inner tag* – Specify whether to add inner tags for ingress untagged packets. If set, the inner tag will be added for the ingress untagged packets and thus the packets egress to the NNI port will be double tagged. If disabled, only s-tag will be added for ingress untagged packets.
Restrictions	Only Administrator and Operator-level users can issue this command. You must be in the Q-in-Q mode.

Example usage:

To config port list 1-4 as NNI port, set outer TPID to 0x88a8:

```
DGS-3700-12:5#config qinq ports 1-4 role nni tpid 0x88a8
Command: config qinq ports 1-4 role nni tpid 0x88a8

Success.

DGS-3700-12:5#
```

show qinq ports

Purpose	Used to show global Q-in-Q and port's Q-in-Q mode status.
Syntax	**show qinq ports <portlist>**
Description	This command is used to show the Q-in-Q configuration for a port, include: port role in Q-in-Q mode, enable/disable to drop the SP-VLAN assignment miss packet, port outer TPID, and the Q-in-Q profile that is applied to the port.
Parameters	*portlist* – Specifies a range of ports to be displayed. If no parameter specified, system will display all ports information.
Restrictions	None.

Example usage:

To show double tagging mode for ports 1-4 of unit 1:

```
DGS-3700-12:5#show qinq ports
Command: show qinq ports

Port   Role    Missdrop  Outer TPID   Use Inner Priority  Add Inner Tag Prev
-----  ------  --------  -----------  ------------------  ------------- ----
1      NNI     Disabled    0x88A8       Disabled            Disabled   On
2      NNI     Disabled    0x88A8       Disabled            Disabled   On
3      NNI     Disabled    0x88A8       Disabled            Disabled   On
4      NNI     Disabled    0x88A8       Disabled            Disabled   On
5      NNI     Disabled    0x88A8       Disabled            Disabled   On
6      NNI     Disabled    0x88A8       Disabled            Disabled   On
7      NNI     Disabled    0x88A8       Disabled            Disabled   On
8      NNI     Disabled    0x88A8       Disabled            Disabled   On
9      UNI     Disabled    0x88A8       Disabled            Disabled   On
10     NNI     Disabled    0x88A8       Disabled            Disabled   On
11     NNI     Disabled    0x88A8       Disabled            Disabled   On
12     NNI     Disabled    0x88A8       Disabled            Disabled   On

DGS-3700-12:5#
```

create vlan_translation ports

Purpose	create VLAN translation rule.
Syntax	**create vlan_translation ports [<portlist> | all] cvid <vidlist> [add| replace] svid <vlanid 1-4094> {priority <value 0-7>}**
Description	This command is used to add translation relationship between C-VLAN and SP-VLAN. On ingress at UNI port, the C-VLAN tagged packets will be translated to SP-VLAN tagged packets by adding or replacing according the configured rule. On egress at this port, the SP-VLAN tag will be recovered to C-VLAN tag or be striped. The priority will be the priority in the SP-VLAN tag if the use_inner_priority flag is disabled for the receipt port. This configuration is only effective for an UNI port. This setting will not be effective when Q-in-Q mode is disabled. Note that the project has the option to implement either the Q-in-Q profile command set or the vlan translation command set. If the project is required to implement the enhanced set of classification method in addition to vlan classification, then Q-in-Q profile command is needed. Otherwise, the vlan translation command set is sufficient.
Parameters	*portlist* – A range of ports on which the SP-VLAN will be translated to C-VLAN. *cvid* – C-VLAN ID to match. *add* – The action indicates to add a tag for the assigned SP-VLAN before the C-VLAN tag. *replace* – The action indicates to replace the C-VLAN tag with the SP VLAN. *svid* – SP-VLAN ID. *priority* – The priority of the s-tag.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create vlan translation rule which assign to add SP-VALN 100 to C-VLAN 1-10 on ports 1-4 and the priority is 4:

```
DGS-3700-12:5# create vlan_translation ports 1-4 cvid 10 add svid 100 priority 4
Command: create vlan_translation ports 1-4 cvid 10 add svid 100 priority 4

Success.

DGS-3700-12:5#
```

delete vlan_translation ports

Purpose	Used to delete pre-created VLAN translation rules
Syntax	**delete vlan_translation ports [<portlist> | all] {cvid <vidlist>}**
Description	The command used to delete pre-created VLAN translation rules.
Parameters	*ports* – A range of ports which the rule will be deleted. *cvid* – Specify C-VLAN range which the rules will be deleted. If no specify the parameter, all rules on the specified ports will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete vlan translation rule on ports 1-4:

```
DGS-3700-12:5# delete vlan_translation ports 1-4
Command: delete vlan_translation ports 1-4

Success.

DGS-3700-12:5#
```

show vlan_translation

Purpose	Used to show pre-created C-VLAN based SP-VLAN assignment rules.
Syntax	**show vlan_translation {ports <portlist>}**
Description	The command used to show pre-created C-VLAN based SP-VLAN assignment rules.
Parameters	*ports* – A range of ports which the rules will be displayed. *cvid* – Specify C-VLAN range which the rules will be displayed. If no specify the parameter, all rules on the specified ports will be displayed. If no parameters specified, all rules will be displayed.
Restrictions	None.

Example usage:

To show vlan_translation rules in the system:

```
DGS-3700-12:5#show vlan_translation
Commands: show vlan_translation
Port        CVID       SPVID      Action      Priority
------      -----       -----     ------      ------
1           10          100        Add         4
1           20          100        Add         5
1           30          200        Add         6
2           10          100        Add         7
2           20          100        Add         1
Total Entries: 5

DGS-3700-12:5#
```

26

RSPAN COMMANDS

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

Command	Parameters
enable rspan	
disable rspan	
create rspan vlan	[vlan_name <vlan_name> | vlan_id <value 1-4094>]
delete rspan vlan	[vlan_name <vlan_name> | vlan_id <value 1-4094>]
config rspan vlan source	[vlan_name <vlan_name>| vlan_id <vlanid 1-4094>] source [add | delete] ports <portlist> mirror [rx | tx | both]
config rspan vlan redirect	vlan [vlan_name <vlan_name>| vlan_id <vlanid 1-4094>] redirect [add | delete] ports < port>
show rspan	{[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}

Each command is listed, in detail, in the following sections.

enable rspan

Purpose	This command is used to enable RSPAN.
Syntax	**enable rspan**
Description	This command controls the RSPAN function. The purpose of RSPAN function is to mirror the packets to the remote switch. The packet travels from the switch where the monitored packet is received, through an intermediate switch, then to the switch where the sniffer is attached. The first switch is also named the source switch. To make the RSPAN work, for the source switch, the RSPAN VLAN source setting must be configured. For the intermediate and the last switch, the RSPAN VLAN redirect setting must be configured. **Note:** RSPAN VLAN mirroring only works when RSPAN is enabled, an RSPAN VLAN has been configured with source ports, and mirror is enabled. RSPAN redirect function will work when RSPAN is enabled and at least one RSPAN VLAN has been configured with redirect ports.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable RSPAN:

```
DGS-3700-12:5#enable rspan
Command: enable rspan

Success.

DGS-3700-12:5#
```

disable rspan

Purpose	This command is used to disable RSPAN
Syntax	**disable rspan**
Description	This command controls the RSPAN function
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable RSPAN:

```
DGS-3700-12:5#disable rspan
Command: disable rspan

Success.

DGS-3700-12:5#
```

create rspan vlan

Purpose	Used to create an RSPAN VLAN
Syntax	**create rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]**
Description	This command is used to create the RSPAN VLAN. Up to 16 RSPAN VLANs can be created.
Parameters	*vlan_name* – Create the RSPAN VLAN by VLAN name. *vlan_id* – Create the RSPAN VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a RSPAN VLAN:

```
DGS-3700-12:5#create rspan vlan vlan_name v3
Command: create rspan vlan vlan_name v3

Success.

DGS-3700-12:5#
```

delete rspan vlan

Purpose	Used to delete a RSPAN VLAN
Syntax	**delete rspan vlan [vlan_name <vlan_name> | vlan_id <value 1-4094>]**
Description	This command is used to delete RSPAN VLANs.
Parameters	*vlan_name* – Delete RSPAN VLAN by VLAN name. *vlan_id* – Delete RSPAN VLAN by VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a RSPAN VLAN:

```
DGS-3700-12:5#delete rspan vlan vlan_name v3
Command: delete rspan vlan vlan_name v3

Success.

DGS-3700-12:5#
```

config rspan vlan source

Purpose	Used by the source switch to configure the source setting for the RSPAN VLAN.
Syntax	**config rspan vlan [vlan_name <vlan_name>| vlan_id <vlanid 1-4094>] source [add | delete] ports <portlist> mirror [rx | tx | both]**
Description	This command configures the source setting for the RSPAN VLAN on the source switch. The output port of the RSPAN mirrored packet will use the same destination port as defined by the mirror command. **Note:** If RSPAN is enabled, the packets mirrored to the destination port are always added with an RSPAN VLAN tag. If mirror is enabled but RSPAN is disabled, the packets mirrored to the destination port may be in tagged form or in untagged form. **Note:** Only one RSPAN VLAN can be configured with source settings.
Parameters	*vlan* – Specify the RSPAN VLAN on the source switch. *vlan_name* – Specify RSPAN VLAN by VLAN name. *vlan_id* – Specify RSPAN VLAN by VLAN ID. *source* – Specify the source settings for the RSPAN VLAN on the source switch. *add* – Add source ports into the RSPAN source. *delete* – Delete source ports from the RSPAN source. *ports* – Specify source portlist to add to or delete from the RSPAN source. *mirror* – Specify the traffic types. *rx* – Only monitor ingress packets. *tx* – Only monitor egress packets. *both* – Monitor both ingress and egress packets.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the rx traffic of port 2 to port 5 mirrored and add vid tag 2 :

```
DGS-3700-12:5#config rspan vlan vlan_name v3 source add ports 2-5 rx
Command: config rspan vlan vlan_name v3 source add ports 2-5 rx

Success.

DGS-3700-12:5#
```

config rspan vlan redirect

Purpose	Used by the intermediate or the last switch to configure the output port for the RSPAN mirrored packet.
Syntax	**config rspan vlan [vlan_name <vlan_name>| vlan_id <vlanid 1-4094>] redirect [add | delete] ports < port>**
Description	This command is used by the intermediate or the last switch to configure the output port of the RSPAN VLAN packets. The redirect command makes sure that the RSPAN VLAN packets can be egress to the redirect ports. In addition to this redirect command, the VLAN setting must be correctly configured to make the RSPAN VLAN work correctly. That is, for the intermediate switch, the redirect port must be a tagged member port of RSPAN VLAN. For the last switch, the redirect port must be either a tagged member port or an untagged member port of the RSPAN VLAN based on the users requirements. If untagged membership is specified, the RSPAN VLAN tag will be removed. The redirect function will only work when RSPAN is enabled. Multiple RSPAN VLANs can be configured with redirect settings at the same time. An RSPAN VLAN can be configured with a source setting and redirect setting at the same time.
Parameters	*vlan* – Specify the RSPAN VLAN on the source switch. *vlan_name* – Specify RSPAN VLAN by VLAN name. *vlan_id* – Specify RSPAN VLAN by VLAN ID. *redirect* – Specify ouptut port for the RSPAN VLAN packets.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure RSPAN VLAN redirection:

```
DGS-3700-12:5# config rspan vlan vlan_name vlan2 redirect add ports 10

Command: config rspan vlan vlan_name vlan2 redirect add ports 10

Success.

DGS-3700-12:5#
```

show rspan

Purpose	Used to display RSPAN configuration.
Syntax	**show rspan {[vlan_name <vlan_name> | vlan_id <vlanid 1-4094>]}**
Description	This command displays the RSPAN configuration.
Parameters	*vlan_name* – Specify the RSPAN VLAN by VLAN name. *vlan_id* – Specify the RSPAN VLAN by VLAN ID.
Restrictions	None.

Example usage:

To display special setting:

```
DGS-3700-12:5#show rspan vlan_id 63

Command: show rspan vlan_id 63

RSPAN  : Enabled

RSPAN VLAN ID : 63
-------------------
Source Ports
RX          : 2-5
TX          : 2-5

Total RSPAN VLAN:1

DGS-3700-12:5#
```

27

STATIC MAC-BASED VLAN COMMANDS

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

Command	Parameters
create mac_based_vlan mac_address	<macaddr> vlan <vlan_name 32>
delete mac_based_vlan	{mac_address <macaddr> vlan <vlan_name 32>}
show mac_based_vlan	{mac <macaddr> | vlan <vlan_name 32>}

Each command is listed, in detail, in the following sections.

create mac_based_vlan

Purpose	Used to create a static mac-based vlan entry.
Syntax	**create mac_based_vlan mac_address <macaddr> vlan <vlan_name 32>**
Description	This command only needs to be supported by the model which supports mac-based VLAN. The user can use this command to create a static mac-based VLAN entry. When a static mac_based_vlan entry is created for a user, the traffic from this user will be able to be serviced under the specified VLAN regardless of the authentiucation function operated on this port. There is a global limitation of the maximum entries supported for the static mac-based entry.
Parameters	*mac_address* – The MAC address. *vlan* – The VLAN to be associated with the MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create mab_local:

```
DGS-3700-12:5# create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: create mac_based_vlan mac_address 00-00-00-00-00-01 vlan default

Success.

DGS-3700-12:5#
```

delete mac_based_vlan

Purpose	Used to delete the static mac-based vlan entry.
Syntax	**delete mac_based_vlan {mac_address <macaddr> vlan <vlan_name 32>}**
Description	This command is used to delete a database entry. If the mac_address and vlan is not specified, all static entries associated with the port will be removed.
Parameters	*mac_address* – The MAC address. *vlan* – The VLAN to be associated with the MAC address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static mac-based-vlan entry:

```
DGS-3700-12:5#delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default
Command: delete mac_based_vlan mac_address 00-00-00-00-00-01 vlan default

Success.

DGS-3700-12:5#
```

show mac_based_vlan

Purpose	Used to show the static or dynamic mac-based vlan entry.
Syntax	**show mac_based_vlan {mac <macaddr> | vlan <vlan_name 32>}**
Description	This command is used to display the static or dynamic MAC-Based VLAN entry.
Parameters	*mac* – The MAC address. *vlan* – The VLAN to be associated with the MAC address.
Restrictions	None.

Example usage:

To display the static or dynamic mac-based-vlan entry:

```
DGS-3700-12:5#show mac_based_vlan
Command: show mac_based_vlan

MAC Address       VLAN        Status         Type
-------------   -----------  -------------  ------------
00-80-e0-14-a7-57   200        Active        Static
00-80-c2-33-c3-45   200        Inactive      Static
00-80-c2-33-c3-45   300        Active        Mac_based Access Control
00-80-c2-33-c3-90   400        Active        802.1x
00-a2-44-17-32-98   500        Active        JWAC

Total Entries : 5

DGS-3700-12:5#
```

28

LINK AGGREGATION COMMANDS

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

Command	Parameters
create link_aggregation	group_id <value 1-6> {type [lacp | static]}
delete link_aggregation	group_id <value 1-6>
config link_aggregation	group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]}(1)
config link_aggregation algorithm	[mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]
show link_aggregation	{group_id <value 1-6> | algorithm}
config lacp_port	<portlist> mode [active | passive]
show lacp_port	{<portlist>}

Each command is listed, in detail, in the following sections.

create link_aggregation

Purpose	Used to create a link aggregation group on the Switch.
Syntax	**create link_aggregation group_id <value 1-6> {type[lacp | static]}**
Description	This command will create a link aggregation group with a unique identifier.
Parameters	*<value>* – Specifies the group ID. The Switch allows up to six link aggregation groups to be configured. The group number identifies each of the groups. *type* – Specify the type of link aggregation used for the group. If the type is not specified the default type is *static*. • *lacp* – This designates the port group as LACP compliant. LACP allows dynamic adjustment to the aggregated port group. LACP compliant ports may be further configured (see config lacp_ports). LACP compliant must be connected to LACP compliant devices. • *static* – This designates the aggregated port group as static. Static port groups can not be changed as easily as LACP compliant port groups since both linked devices must be manually configured if the configuration of the trunked group is changed. If static link aggregation is used, be sure that both ends of the connection are properly configured and that all ports have the same speed/duplex settings.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a link aggregation group:

```
DGS-3700-12:5#create link_aggregation group_id 2
Command: create link_aggregation group_id 2

Success.

DGS-3700-12:5#
```

delete link_aggregation

Purpose	Used to delete a previously configured link aggregation group.
Syntax	**delete link_aggregation group_id <value 1-6>**
Description	This command is used to delete a previously configured link aggregation group.
Parameters	*<value 1-6>* – Specifies the group ID. The Switch allows up to six link aggregation groups to be configured. The group number identifies each of the groups.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete link aggregation group:

```
DGS-3700-12:5#delete link_aggregation group_id 2
Command: delete link_aggregation group_id 2

Success.

DGS-3700-12:5#
```

config link_aggregation

Purpose	Used to configure a previously created link aggregation group.
Syntax	**config link_aggregation group_id <value 1-6> {master_port <port> | ports <portlist> | state [enable | disable]}(1)**
Description	This command allows users to configure a link aggregation group that was created with the **create link_aggregation** command above.
Parameters	*group _id <value 1-6>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *master_port <port>* – Master port ID. Specifies which port (by port number) of the link aggregation group will be the master port. All of the ports in a link aggregation group will share the port configuration with the master port. *ports <portlist>* – Specifies a port or range of ports that will belong to the link aggregation group. *state [enable | disable]* – Allows users to enable or disable the specified link aggregation group.
Restrictions	Only Administrator and Operator-level users can issue this command. Link aggregation groups may not overlap.

Example usage:

To define a load-sharing group of ports, group-id 1,master port 5 with group members ports 5-7, 9:

```
DGS-3700-12:5#config link_aggregation group_id 1 master_port 5 ports 5-7, 9
Command: config link_aggregation group_id 1 master_port 5 ports 5-7, 9

Success.

DGS-3700-12:5#
```

config link_aggregation algorithm

Purpose	Used to configure the link aggregation algorithm.
Syntax	**config link_aggregation algorithm [mac_source | mac_destination | mac_source_dest | ip_source | ip_destination | ip_source_dest]**
Description	This command configures the part of the packet examined by the Switch when selecting the egress port for transmitting load-sharing data. This feature is only available using the address-based load-sharing algorithm.
Parameters	*mac_source* – Indicates that the Switch should examine the MAC source address. *mac_destination* – Indicates that the Switch should examine the MAC destination address. *mac_source_dest* – Indicates that the Switch should examine the MAC source and destination addresses. *ip_source* – Indicates that the Switch should examine the IP source address. *ip_destination* – Indicates that the Switch should examine the IP destination address. *ip_source_dest* – Indicates that the Switch should examine the IP source address and the destination address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure link aggregation algorithm for mac-source-dest:

```
DGS-3700-12:5#config link_aggregation algorithm mac_source_dest
Command: config link_aggregation algorithm mac_source_dest

Success.

DGS-3700-12:5#
```

show link_aggregation

Purpose	Used to display the current link aggregation configuration on the Switch.
Syntax	**show link_aggregation {group_id <value 1-6> | algorithm}**
Description	This command will display the current link aggregation configuration of the Switch.
Parameters	*<value 1-6>* – Specifies the group ID. The Switch allows up to 6 link aggregation groups to be configured. The group number identifies each of the groups. *algorithm* – Allows users to specify the display of link aggregation by the algorithm in use by that group.
Restrictions	None.

Example usage:

To display Link Aggregation configuration:

```
DGS-3700-12:5#show link_aggregation
Command: show link_aggregation

Link Aggregation Algorithm = MAC-Source-Dest

Group ID        : 3
Type            : TRUNK
Master Port     :
Member Port     :
Active Port     :
Status          : Disabled
Flooding Port   :

Total Entries : 1

DGS-3700-12:5#
```

config lacp_port

Purpose	Used to configure settings for LACP compliant ports.
Syntax	**config lacp_port <portlist> mode [active | passive]**
Description	This command is used to configure ports that have been previously designated as LACP ports (see **create link_aggregation**).
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *mode* – Select the mode to determine if LACP ports will process LACP control frames. • *active* – Active LACP ports are capable of processing and sending LACP control frames. This allows LACP compliant devices to negotiate the aggregated link so the group may be changed dynamically as needs require. In order to utilize the ability to change an aggregated port group, that is, to add or subtract ports from the group, at least one of the participating devices must designate LACP ports as active. Both devices must support LACP. • *passive* – LACP ports that are designated as passive cannot process LACP control frames. In order to allow the linked port group to negotiate adjustments and make changes dynamically, at one end of the connection must have “active” LACP ports (see above).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure LACP port mode settings:

```
DGS-3700-12:5#config lacp_port 1-12 mode active
Command: config lacp_port 1-12 mode active

Success.

DGS-3700-12:5#
```

show lacp_port

Purpose	Used to display current LACP port mode settings.
Syntax	**show lacp_port {<portlist>}**
Description	This command will display the LACP mode settings as they are currently configured.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. If no parameter is specified, the system will display the current LACP status for all ports.
Restrictions	None.

Example usage:

To display LACP port mode settings:

```
DGS-3700-12:5#show lacp_port 1-10
Command: show lacp_port 1-10

Port      Activity
------     --------
1          Active
2          Active
3          Active
4          Active
5          Active
6          Active
7          Active
8          Active
9          Active
10         Active

DGS-3700-12:5#
```

29

TRAFFIC SEGMENTATION COMMANDS

Traffic segmentation allows users to further sub-divide VLANs into smaller groups of ports that will help to reduce traffic on the VLAN. The VLAN rules take precedence, and then the traffic segmentation rules are applied.

Command	Parameters
config traffic_segmentation	[<portlist> | all] forward_list [null | all | <portlist>]
show traffic_segmentation	<portlist>

Each command is listed, in detail, in the following sections.

config traffic_segmentation

Purpose	Used to configure traffic segmentation on the Switch.
Syntax	**config traffic_segmentation [<portlist> | all] forward_list [null | all | <portlist>]**
Description	This command is used to configure traffic segmentation on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports that will be configured for traffic segmentation. *all* – Specifies all the ports that will be configured for traffic segmentation. *forward_list* – Specifies a range of ports that will receive forwarded frames from the ports specified in the portlist, above. • *null* – No ports are specified. • *all* – All ports are specified. • *<portlist>* – Specifies a range of ports for the forwarding list. This list must be on the same Switch previously specified for traffic segmentation (i.e. following the *<portlist>* specified above for **config traffic_segmentation**).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ports 1 through 10 to be able to forward frames to port 1 through 5:

```
DGS-3700-12:5#config traffic_segmentation 1-10 forward_list 1-5
Command: config traffic_segmentation 1-10 forward_list 1-5

Success.

DGS-3700-12:5#
```

show traffic_segmentation

Purpose	Used to display the current traffic segmentation configuration on the Switch.
Syntax	**show traffic_segmentation <portlist>**
Description	This command is used to display the current traffic segmentation configuration on the Switch.
Parameters	*<portlist>* – Specifies a port or range of ports for which the current traffic segmentation configuration on the Switch will be displayed.
Restrictions	None.

Example usage:

To display the current traffic segmentation configuration on the Switch:

```
DGS-3700-12:5#show traffic_segmentation
Command: show traffic_segmentation

Traffic Segmentation Table

Port  Forward Portlist
----  ------------------------------------------------------------
1      1-12
2      1-12
3      1-12
4      1-12
5      1-12
6      1-12
7      1-12
8      1-12
9      1-12
10     1-12
11     1-12
12     1-12

DGS-3700-12:5#
```

30

BPDU TUNNELLING COMMANDS

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

Command	Parameters
config bpdu_tunnel ports	[<portlist> | all] type [tunnel {stp|gvrp}|uplink|none]
show bpdu_tunnel	
enable bpdu_tunnel	
disable bpdu_tunnel	

Each command is listed, in detail, in the following sections.

config bpdu_tunnel ports

Purpose	Used to configure BPDU Tunnelling type ports.
Syntax	**config bpdu_tunnel ports [<portlist> | all] type [tunnel {stp|gvrp}|uplink|none]**
Description	This command is used to configure BPDU Tunnelling type ports. When the device is operated with Q-in-Q enabled, the DA will be replaced by the tunnel multicast address, and the BPDU will be tagged with the tunnel VLAN based on the Q-in-Q VLAN configuration and the tunnel/uplink settings. When the device is operated without Q-in-Q enabled, the BPDU will have its DA replaced by the tunnel multicast address and be transmitted out based on the VLAN configuration and the tunnel/uplink settings. The tunnel multicast address for STP BPDU is 01-05-5d-00-00-00. The tunnel multicast address for GVRP BPDU is 01-05-5d-00-00-21.
Parameters	*ports* – Specifies the ports on which the BPDU Tunnelling will be enabled or disabled. *type* – Specifies the type of ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the BPDU tunnelling ports:

```
DGS-3700-12:5#config bpdu_tunnel ports 1-4 type tunnel stp
Command: config bpdu_tunnel ports 1-4 type tunnel stp

Success.

DGS-3700-12:5#
```

show bpdu_tunnel

Purpose	Used to show BPDU Tunnelling global state, tunnel destination MAC address and ports state.
Syntax	**show bpdu_tunnel**
Description	This command is used to show BPDU Tunnelling global state, tunnel destination MAC address and ports state.
Parameters	None.
Restrictions	None.

Example usage:

To display the BPDU tunnelling state of all ports:

```
DGS-3700-12:5#show bpdu_tunnel
Command: show bpdu_tunnel

 BPDU Tunnel : Disabled
 STP Tunnel Multicast Address : 01-05-5D-00-00-00
 STP Tunnel Port : 1-4
 GVRP Tunnel Multicast Address : 01-05-5D-00-00-21
 GVRP Tunnel Port :
 Uplink Port :

DGS-3700-12:5#
```

enable bpdu_tunnel

Purpose	Used to enable the BPDU Tunnelling function.
Syntax	**enable bpdu_tunnel**
Description	This command is used to enable the BPDU Tunnelling function. By default, the BPDU Tunneling is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable bpdu_tunnel:

```
DGS-3700-12:5#enable bpdu_tunnel
Command: enable bpdu_tunnel

Success.

DGS-3700-12:5#
```

disable bpdu_tunnel

Purpose	Used to disable the BPDU Tunnelling function.
Syntax	**disable bpdu_tunnel**
Description	This command is used to disable the BPDU Tunneling function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable bpdu_tunnel:

```
DGS-3700-12:5#disable bpdu_tunnel
Command: disable bpdu_tunnel

Success.

DGS-3700-12:5#
```

31

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	Parameters
config igmp_snooping	[vlan_name <vlan_name 32> | vlanid <vidlist> |all] { state [enable|disable] | fast_leave [enable|disable] | report_suppression [enable | disable]}(1)
config igmp_snooping querier	[vlan_name <vlan_name 32> | vlanid <vidlist> |all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> |last_member_query_interval <sec 1-25> | state [enable|disable] |version <value 1-3>}(1)
enable igmp_snooping	
show igmp_snooping	{[vlan <vlan_name 32> | vlanid <vidlist>]}
disable igmp_snooping	
show igmp_snooping group	{[vlan <vlan_name 32> | vlanid <vidlist> | ports <portlist>] {<ipaddr>}} {data_driven}
show igmp_snooping rate_limit	[ports <portlist>|vlanid <vlanid_list>]
config igmp_snooping rate_limit	[ports <portlist>|vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show igmp_snooping forwarding	{[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show igmp_snooping static_group	{[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipaddr >}
create igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
delete igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>
config igmp_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>
show igmp_snooping statistic counter	[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
clear igmp_snooping statistic counter	
config router_ports	[vlan <vlan_name 32> | vlanid <vlanid_list>] [add |delete] <portlist>
config router_ports_forbidden	[vlan <vlan_name 32> | vlanid <vlanid_list>] [add |delete] <portlist>
show router ports	[vlan <vlan_name 32> | vlanid <vlanid_list> |all] {[static |dynamic|forbidden]}
config igmp_snooping data_driven_learning max_learned_entry	<value 1-1024>
config igmp_snooping data_driven_learning	[all | vlan_name <vlan_name> | vlanid <vidlist>] { state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)
clear igmp_snooping data_driven_group	[all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr>| all]]

Each command is listed, in detail, in the following sections.

config igmp_snooping

Purpose	Used to configure IGMP snooping on the Switch.
Syntax	**config igmp_snooping [vlan_name <vlan_name 32> | vlanid <vidlist> |all] { state [enable|disable] | fast_leave [enable|disable] | report_suppression [enable | disable]}(1)**
Description	This command allows the user to configure IGMP snooping on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which IGMP snooping is to be configured. *<vidlist>* – The VIDs of the VLAN for which IGMP snooping is to be configured. *state [enable | disable]* – Allows users to enable or disable IGMP snooping for the specified VLAN. *fast_leave [enable|disable]* – Allows users to enable or disable IGMP snooping fast leave for the specified VLAN. *report_suppression [enable|disable]* – Allows users to enable or disable IGMP snooping report suppression for the specified VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure IGMP snooping:

```
DGS-3700-12:5#config igmp_snooping vlan default state enable fast_leave enable
report_suppression disable
Command: config igmp_snooping vlan default state enable fast_leave enable
report_suppression disable

Success.

DGS-3700-12:5#
```

config igmp_snooping querier

Purpose	Used to configure the the time in seconds between general query transmissions, the maximum time in seconds to wait for reports from members and the permitted packet loss that guarantees IGMP snooping.
Syntax	**config igmp_snooping querier [vlan_name <vlan_name 32> | vlanid <vidlist> |all] {query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> |last_member_query_interval <sec 1-25> | state [enable|disable] |version <value 1-3>}(1)**
Description	This command is used to configure IGMP snooping querier.
Parameters	*vlan_name* – The name of the VLAN for which IGMP snooping querier is to be configured. *<vidlist>* – The VIDs of the VLAN for which IGMP snooping is to be configured. *query_interval* – Specifies the amount of time in seconds between general query transmissions. the default setting is *125* seconds. *max_response_time* – The maximum time in seconds to wait for reports from members. The default setting is *10* seconds. *robustness_variable* – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following IGMP message intervals: • Group member interval – Amount of time that must pass before a multicast router decides there are no more members of a group on a network. This interval is calculated as follows: (robustness variable x query interval) + (1 x query response interval). • Other querier present interval – Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable x query interval) + (0.5 x query response interval). • Last member query count – Number of group-specific queries sent before the router assumes there are no local members of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to *2*. You might want to increase this value if you expect a subnet to be lossy. *last_member_query_interval* – The maximum amount of time between group-specific query messages, including those sent in response to leave-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last member of a group. *state* – If the state is enable, it allows the switch to be selected as a IGMP Querier (sends IGMP query packets). It the state is disabled, then the switch can not play the role as a querier. Note that if the Layer 3 router connected to the switch provide only the IGMP proxy function but not provide the mutlicast routing function, then this state must be configured as disabled. Otherwise, if the Layer 3 router is not selected as the querier, it will not send the IGMP query packet. Since it will not also send the multicast-routing protocol packet, the port will be timed out as a router port. *version* – The version of the IGMP Query sent by the switch.
Restrictions	Only Administrator or Operator-level users can issue this command.

Example usage:

To configure the IGMP snooping querier:

```
DGS-3700-12:5#config igmp_snooping querier vlan default query_interval 125 state enable
Command: config igmp_snooping querier vlan default query_interval 125 state enable

Success.

DGS-3700-12:5#
```

config router_ports

Purpose	Used to configure ports as router ports.
Syntax	**config router_ports [vlan <vlan_name 32> | vlanid <vidlist>]**
Description	This command allows users to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *<vid_list>* – The VIDs of the VLAN on which the router port resides. *[add|delete]* – Specifies whether to add or delete router ports of the specified VLAN. *<portlist>* – Specifies a port or range of ports that will be configured as router ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up static router ports:

```
DGS-3700-12:5#config router_ports vlan default add 1-10
Command: config router_ports vlan default add 1-10

Success.

DGS-3700-12:5#
```

config router_ports_forbidden

Purpose	Used to configure ports as forbidden multicast router ports.
Syntax	**config router_ports_forbidden [vlan <vlan_name 32> | vlanid <vidlist>] [add|delete] <portlist>**
Description	This command allows designation of a port or range of ports as being forbidden to multicast-enabled routers. This will ensure that multicast packets will not be forwarded to this port – regardless of protocol, etc.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *<vid_list>* – The VIDs of the VLAN on which the forbidden router port resides. *[add* | *delete]* – Specifies whether to add or delete forbidden router ports of the specified VLAN. *<portlist>* – Specifies a range of ports that will be configured as forbidden router ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up forbidden router ports:

```
DGS-3700-12:5#config router_ports_forbidden vlan default add 2-10
Command: config router_ports_forbidden vlan default add 2-10

Success.

DGS-3700-12:5#
```

enable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**enable igmp_snooping**
Description	This command allows users to enable IGMP snooping on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IGMP snooping on the Switch:

```
DGS-3700-12:5#enable igmp_snooping
Command: enable igmp_snooping

Success.

DGS-3700-12:5#
```

disable igmp_snooping

Purpose	Used to enable IGMP snooping on the Switch.
Syntax	**disable igmp_snooping**
Description	This command disables IGMP snooping on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable IGMP snooping on the Switch:

```
DGS-3700-12:5#disable igmp_snooping
Command: disable igmp_snooping

Success.

DGS-3700-12:5#
```

show igmp_snooping

Purpose	Used to show the current status of IGMP snooping on the Switch.
Syntax	**show igmp_snooping {[vlan <vlan_name 32>** **| vlanid <vlanid_list>] }**
Description	This command will display the current IGMP snooping configuration on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view the IGMP snooping configuration. *<vlanid_list>* – The VIDs of the VLAN for which to view the IGMP snooping configuration.
Restrictions	None.

Example usage:

To show IGMP snooping:

```
DGS-3700-12:5#show igmp_snooping
Command: show igmp_snooping

 IGMP Snooping Global State              : Enabled
 Data Driven Learning Max Entries        : 128

 VLAN Name                     : default
 Query Interval                : 125
 Max Response Time             : 10
 Robustness Value              : 2
 Last Member Query Interval    : 1
 Querier State                 : Disable
 Querier Role                  : Non-Querier
 Querier IP                    : 0.0.0.0
 Querier Expiry Time           : 0 secs
 State                         : Disable
 Fast Leave                    : Disable
 Report Suppression            : Enable
 Rate Limit                    : No Limitation
 Version                       : 3
 Data Driven Learning State    : Enable
 Data Driven Learning Aged Out : Disable
 Data Driven Group Expiry Time : 260

Total Entries: 1


DGS-3700-12:5#
```

show router_ports

Purpose	Used to display the currently configured router ports on the Switch.
Syntax	**show router_ports [vlan <vlan_name 32>| vlanid <vidlist>|all] {[static | dynamic | forbidden]}**
Description	This command will display the router ports currently configured on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the router port resides. *<vid_list>* – The VIDs of the VLAN on which the router port resides. *all* – All the IGMP router ports will be displayed. *static* – Displays router ports that have been statically configured. *dynamic* – Displays router ports that have been dynamically configured. *forbidden* – Displays router ports that are forbidden.
Restrictions	None.

Example usage:

To display the router ports.

```
DGS-3700-12:5#show router_ports all
Command: show router_ports all

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

VLAN Name                : v1
Static router port       :
Dynamic router port      :
  Router IP              :
Forbidden router port    :

VLAN Name                : RG
Static router port       :
Dynamic router port      :
  Router IP              :
Forbidden router port    :

Total Entries: 3

DGS-3700-12:5#
```

show igmp_snooping group

Purpose	Used to display the current IGMP snooping configuration on the Switch.
Syntax	**show igmp_snooping group {[vlan <vlan_name 32> | vlanid <vidlist> | ports <portlist>] {<ipaddr>}} {data_driven}**
Description	This command will display the current IGMP setup currently configured on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view IGMP snooping group information. *<vlanid_list>* – The VIDs of the VLAN for which to view IGMP snooping group information. *<portlist>* – The list of ports for which to view IGMP snooping group information. *<ipaddr>* – To view the information of this specified group. *data_driven* – To view the groups learnt by data driven only. If no parameter is specified, the system will display all current IGMP snooping groups.
Restrictions	None.

Example usage:

To view the current IGMP snooping group:

```
DGS-3700-12:5#show igmp_snooping group
Command: show igmp_snooping group

Source/Group      : NULL/224.1.1.1
VLAN Name/VID     : default/1
Member Ports      : 12
Up Time           : 62
Expiry Time       : 198
Filter Mode       : EXCLUDE

Source/Group      : NULL/224.1.1.2
VLAN Name/VID     : default/1
Member Ports      : 11
Up Time           : 72
Expiry Time       : 188
Filter Mode       : EXCLUDE

Source/Group      : 29.1.1.1/229.1.1.1
VLAN Name/VID     : default/1
Member Ports      : 12
Up Time           : 3
Expiry Time       : 257
Filter Mode       : INCLUDE

Source/Group      : 29.1.1.2/229.1.1.1
VLAN Name/VID     : default/1
Member Ports      : 12
Up Time           : 3
Expiry Time       : 257
Filter Mode       : INCLUDE

Source/Group      : 29.1.1.3/229.1.1.1
VLAN Name/VID     : default/1
Member Ports      : 12
Up Time           : 3
Expiry Time       : 257
Filter Mode       : INCLUDE

Source/Group      : 29.1.1.4/229.1.1.1
VLAN Name/VID     : default/1
Member Ports      : 12
Up Time           : 3
Expiry Time       : 257
Filter Mode       : INCLUDE

Total Entries : 6


DGS-3700-12:5#
```

show igmp_snooping rate_limit

Purpose	Used to show rate limitation.
Syntax	**show igmp_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>]**
Description	This command is used to display the rate of IGMP control packet that is allowed per port or VLAN.
Parameters	*<portlist>* – Specifies a port or range of ports that will be displayed. *<vlanid_list>* – Specifies a VLAN or range of VLANs that will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show rate limitation:

```
DGS-3700-12:5#show igmp_snooping rate_limit ports 1
Command: show igmp_snooping rate_limit ports 1

 Port      Rate Limitation
 --------  --------------
 1         No Limitation

Total Entries: 1

DGS-3700-12:5#
```

config igmp_snooping rate_limit

Purpose	Used to show rate limitation.
Syntax	**config igmp_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>] [<value 1-1000> | no_limit]**
Description	This command is used to configure the rate of IGMP control packets that are allowed per port or VLAN.
Parameters	*<portlist>* – Specifies a port or range of ports that will be displayed. *<vlanid_list>* – Specifies a VLAN or range of VLANs that will be displayed. *<value 1-1000>* – Specifies the rate of IGMP control packet that the switch can process on a specific port. The rate is specified in packets per second. The packets that exceeds the limited rate will be dropped. The default setting is no_limit. *no_limit* – Allows users to configure the rate limitation to no limit.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure rate limitation:

```
DGS-3700-12:5#config igmp_snooping rate_limit ports 1 100
Command: config igmp_snooping rate_limit ports 1 100

Success.

DGS-3700-12:5#
```

show igmp_snooping forwarding

Purpose	Used to display the current IGMP snooping forwarding information on the Switch.
Syntax	**show igmp_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}**
Description	This command will display the current IGMP forwarding information on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view IGMP snooping forwarding information. If not specified, all VLAN's IGMP snooping forwarding information will be displayed. *<vlanid_list>* – The list of the VLAN IDs for which to view IGMP snooping forwarding information. If not specified, all VLAN's IGMP snooping forwarding information will be displayed.
Restrictions	None.

Example usage:

To view the current IGMP snooping forwarding information:

```
DGS-3700-12:5#show igmp_snooping forwarding
Command: show igmp_snooping forwarding


 VLAN Name                 : default
 Source IP                 : *
 Multicast Group           : 225.1.1.1
 Port Member               : 3

 Total Entries : 1
```

show igmp_snooping static_group

Purpose	Used to display the current IGMP snooping static group information on the Switch.
Syntax	**show igmp_snooping static_group {[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipaddr >}**
Description	This command is used to display the current IGMP snooping static group information on the Switch.
Parameters	<*vlan_name 32*> – The name of the VLAN for which to view IGMP snooping static group information, if not specified, all static groups will be displayed. <*vlanid_list*> – The list of the VLAN IDs for which to view IGMP snooping static group information, if not specified, all static groups will be displayed. < *ipaddr* > – The static group address for which to view IGMP snooping static group information.
Restrictions	None.

Example usage:

To view the current IGMP snooping static group information:

```
DGS-3700-12:5#show igmp_snooping static_group
Command: show igmp_snooping static_group

VLAN ID/Name                     IP Address       Static Member Ports
-------------------------------  ---------------  -------------------
1/default                        225.1.1.1        1-3

 Total Entries : 1

DGS-3700-12:5#
```

create igmp_snooping static_group

Purpose	Used to display the current IGMP snooping static group information on the Switch.
Syntax	**create igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr>**
Description	This command allows you to create an IGMP snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when IGMP snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the IGMP protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V2 IGMP operation. The Reserved IP multicast address 224.0.0.X must be excluded from the configured group. The VLAN must be created first before a static group can be created.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to create IGMP snooping static group information. *<vlanid_list>* – The list of the VLAN IDs for which to create IGMP snooping static group information. *< ipaddr >* – The static group address for which to create IGMP snooping static group information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static group 226.1.1.1 for VID 1:

```
DGS-3700-12:5#create igmp_snooping static_group vlanid 1 226.1.1.1
Command: create igmp_snooping static_group vlanid 1 226.1.1.1

Success.

DGS-3700-12:5#
```

delete igmp_snooping static_group

Purpose	Used to delete the current IGMP snooping static group on the Switch.
Syntax	**delete igmp_snooping static_group [vlan <vlan_name 32> | vlanid < *vlanid_list* >] <ipaddr>**
Description	This command is used to delete an IGMP snooping static group will not affect the IGMP snooping dynamic member ports of a group.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to delete IGMP snooping static group information. *<vlanid_list>* – The list of the VLAN IDs for which to delete IGMP snooping static group information. *< ipaddr >* – The static group address for which to delete IGMP snooping static group information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static group 226.1.1.1 on VID 1:

```
DGS-3700-12:5#delete igmp_snooping static_group vlanid 1 226.1.1.1
Command: delete igmp_snooping static_group vlanid 1 226.1.1.1

Success.

DGS-3700-12:5#
```

config igmp_snooping static_group

Purpose	Used to configure the current IGMP snooping static group on the Switch.
Syntax	**config igmp_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipaddr> [add | delete] <portlist>**
Description	This command is used to add or delete ports to/from the given static group.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to configure IGMP snooping static group information. *<vlanid_list>* – The list of the VLAN IDs for which to configure IGMP snooping static group information. *< ipaddr >* – The static group address for which to configure IGMP snooping static group information. *[add | delete] <portlist>* – Portlist to add or delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add port 5 to static group 226.1.1.1 on VID 1:

```
DGS-3700-12:5#config igmp_snooping static_group vlanid 1 226.1.1.1 add 5
Command: config igmp_snooping static_group vlanid 1 226.1.1.1 add 5

Success.

DGS-3700-12:5#
```

show igmp_snooping statistic counter

Purpose	Used to view the current IGMP snooping statistics on the Switch.
Syntax	**show igmp_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]**
Description	This command is used to view this information, snooping must be enabled first.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view IGMP snooping statistic counter. *<vlanid_list>* – The list of the VLAN IDs for which to view IGMP snooping statistic counter. *<portlist>* – The list of the ports for which to view IGMP snooping statistic counter.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view IGMP snooping statistic on VID 1:

```
DGS-3700-12:5#show igmp_snooping statistic counter vlanid 1
Command: show igmp_snooping statistic counter vlanid 1


VLAN Name         : default
------------------------------------------------
Group Number      : 1

Receive Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Multicast VLAN        : 0

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0
      Dropped By Rate Limitation       : 0
      Dropped By Max Group Limitation  : 0
      Dropped By Group Filter          : 0
      Dropped By Multicast VLAN        : 0

Transmit Statistics
    Query
      IGMP v1 Query                    : 0
      IGMP v2 Query                    : 0
      IGMP v3 Query                    : 14
      Total                            : 14

    Report & Leave
      IGMP v1 Report                   : 0
      IGMP v2 Report                   : 0
      IGMP v3 Report                   : 0
      IGMP v2 Leave                    : 0
      Total                            : 0

 Total Entries : 1


DGS-3700-12:5#
```

clear igmp_snooping statistic counter

Purpose	Used to clear the current IGMP snooping statistic on the Switch.
Syntax	**clear igmp_snooping statistic counter**
Description	This command is used to clear all IGMP snooping statistic counters.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear IGMP snooping statistic counter:

```
DGS-3700-12:5#clear igmp_snooping statistic counter
Command: clear igmp_snooping statistic counter

Success.

DGS-3700-12:5#
```

config igmp_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the max number of groups that can be learned by data driven.
Syntax	**config igmp_snooping data_driven_learning max_learned_entry <value 1-1024>**
Description	This command is used to configure the maximum number of groups that can be learned by data driven. When the table is full, the system will stop learning the new data-driven groups. Traffic for the new groups will be dropped.
Parameters	*<value 1-1024 >* – The max number of groups that can be learned by data driven.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the max number of groups that can be learned by data driven:

```
DGS-3700-12:5#config igmp_snooping data_driven_learning max_learned_
entry 100
Command: config igmp_snooping data_driven_learning max_learned_entry 100

Success.

DGS-3700-12:5#
```

config igmp_snooping data_driven_learning

Purpose	Used to configure the data driven learing of a IGMP snooping group.
Syntax	**config igmp_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] { state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)**
Description	This command is used to configure the data driven learning of an IGMP snooping group. When data-driven learning is enabled for the VLAN, the switch receives the IP multicast traffic on this VLAN, and an IGMP snooping group will be created. The learning of an entry is not activated by IGMP membership registration, but by the traffic. For an ordinary IGMP snooping entry, the IGMP protocol will take care that the ageing out of the entry. For a data-driven entry, the entry can be specified so that it doesnt ageout or ageout by the aged timer. When data driven learning is enabled, and data driven table is not full, the multicast filtering mode for all ports are ignored. The multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to the multicast filtering mode. **Note:** If a data-driven group is created and IGMP member ports are learned later, the entry will become an ordinary IGMP snooping entry. That is, the ageing out mechanism will follow the ordinary IGMP snooping entry.
Parameters	*all* – Configure all VLAN's IGMP Snooping configuration. *vlan_name <vlan_name 32>* – The name of the VLAN for which IGMP snooping data driven learning is to be configured. *vlanid <vlanid_list>* – The VID of the VLAN for which IGMP snooping data driven learning is to be configured. *state [enable | disable]* – Allows users to enable or disable IGMP snooping data driven learning for the specified VLAN. *aged_out [enable|disable]* – Allows users to enable or disable the aged_out time of the IGMP Snooping data driven learning for the specified VLAN. *expiry_time <sec 1-65535>* – Allows users to set the time that an IGMP Snooping data driven learning group will expire for the specified VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable data driven learning on VLAN default:

```
DGS-3700-12:5# config igmp_snooping data_driven_learning vlan_name default state
enable aged_out enable expiry_time 270

Command: config igmp_snooping data_driven_learning vlan_name default state enable
aged_out enable expiry_time 270

Success.

DGS-3700-12:5#
```

clear igmp_snooping data_driven_group

Purpose	Used to delete the IGMP snooping group learned by data driven.
Syntax	**clear igmp_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr>| all]]**
Description	This command is used to delete the IGMP snooping group learned by data driven.
Parameters	*all* – Delete all groups learnt by data driven. *vlan_name* <*vlan_name 32*> – The name of the VLAN for which IGMP snooping data driven learning group is to be deleted. *vlanid* <*vlanid_list*> – The VID of the VLAN for which IGMP snooping data driven learning group is to be deleted. <*ipaddr*> – The group address for which IGMP snooping data driven learning group is to be deleted on the specified VLAN. <*all*> – All groups learnt by data driven on the specified VLAN will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all groups learnt by data driven on VLAN default:

```
DGS-3700-12:5#clear igmp_snooping data_driven_group vlan_name default all
Command: clear igmp_snooping data_driven_group vlan_name default all

Success.

DGS-3700-12:5#
```

32

IGMP MULTICAST VLAN COMMANDS

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

Command	Parameters
create igmp_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config igmp_snooping multicast_vlan	<vlan_name 32> { [add | delete] [member_port <portlist> | source_port <portlist> |tag_member_port <portlist>] | state [enable|disable] |replace_source_ip <ipaddr>}(1)
config igmp_snooping multicast_vlan_group	<vlan_name 32> [add | delete] profile_name <profile_name 1-32> <vlan_name 32>
show igmp_snooping multicast_vlan_group	{< vlan_name 32> }
delete igmp_snooping multicast_vlan	<vlan_name 32>
enable igmp_snooping multicast_vlan	
disable igmp_snooping multicast_vlan	
show igmp_snooping multicast_vlan	{<vlan_name 32>}
create igmp_snooping multicast_vlan_group_profile	<profile_name 1-32>
config igmp_snooping multicast_vlan_group_profile	<profile_name 1-32> [add | delete] <mcast_address_list>
delete igmp_snooping multicast_vlan_group_profile	[profile_name <profile_name 1-32> |all]
show igmp_snooping multicast_vlan_group_profile	{<profile_name 1-32>}
config igmp_snooping multicast_vlan forward_unmatched	[disable | enable]

Each command is listed, in detail, in the following sections.

create igmp_snooping multicast_vlan

Purpose	Used to create an IGMP multicast VLAN
Syntax	**create igmp_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>.**
Description	This command is used to create an IGMP multicast_vlan. Multiple multicast VLAN can be configured. The IGMP multicast VLAN being created can not exist in the 1Q VLAN database. Multiple IGMP multicast VLAN can be created. The IGMP multicast VLAN snooping function co-exist with the 1Q VLAN snooping function.
Parameters	*<vlan_name>* – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. *vlanid* – The VLAN ID of the multicast VLAN to be create. The range is 2-4094
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create IGMP multicast VLAN RG 11:

```
DGS-3700-12:5# create igmp_snooping multicast_vlan RG 11
Command: create igmp_snooping multicast_vlan RG 11

Success.
DGS-3700-12:5#
```

config igmp_snooping multicast_vlan

Purpose	Used to configure the parameter of the specific IGMP multicast VLAN.
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 <ipaddr>}(1)**
Description	This command allows you to add a member port, add a tag member port, and add a source port to the port list. The member port will automatically become the untagged member of the IGMP multicast VLAN, the tag member port and the source port will automatically become the tagged member of the IGMP multicast VLAN. To change the port list, the new port list will replace the previous port list if the add or delete is not specified. The member port list and source port list can not overlap. However, the member port of one IGMP multicast VLAN can overlap with another IGMP multicast VLAN. The IGMP multicast VLAN must be created first before configuration.
Parameters	*<vlan_name>* – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. *Member_port* – A range of member ports to add to the multicast VLAN. They will become the untagged member port of the IGMP multicast VLAN. *tag_member_port* – Specifies the tagged member port of the IGMP multicast VLAN. *source_port* – A range of source ports to add to the multicast VLAN. *state* – enable or disable multicast VLAN for the chosen VLAN. *replace_source_ip* – With the IGMP snooping function, the IGMP report packet sent by the host will be forwarded to the source port. Before forwarding of the packet, the source IP address in the join packet needs to replaced by this IP address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure an IGMP multicast VLAN:

```
DGS-3700-12:5#config igmp_snooping multicast_vlan v1 add member_port 1,3 state enable
Command: config igmp_snooping multicast_vlan v1 add member_port 1,3 state enable

Success.

DGS-3700-12:5#
```

config igmp_snooping multicast_vlan_group

Purpose	Used to configure the multicast group which will be learned with the specific IGMP multicast VLAN.
Syntax	**<vlan_name 32> [add | delete] profile_name <profile_name 1- 32**
Description	This command is used to configure the multicast group which will be learned by the specific IGMP multicast VLAN. There are two cases that need to be considered. The join packet will be learned with the IGMP multicast VLAN that contains the destination multicast group. If the destination multicast group of the join packet can not be classified into any IGMP multicast VLAN that this port belongs to, then the join packet will be learned with the natural VLAN of the packet. When an IGMP packet is received, first, it will check whether to be processed by the IGMP snooping. If the IGMP snooping for the classified VLAN of this IGMP packet is enabled, it will be processed based on IGMP snooping function. If the IGMP snooping for the classified VLAN of this IGMP packet is disabled, then it will be checked whether to be processed by the IGMP Multicast VLAN function. There are some cases when an IGMP packet can be processed by IGMP Multicast VLAN. If there are no profiles systemwise, and there is only one IGMP Multicast VLAN, then this IGMP packet will be associated with this only IGMP Multicast VLAN. If the packet is a tagged packet, the packet will be matched against the profile on this VLAN. If matched, the packet will be associated with this VLAN. Otherwise, the packet is an unmatched packet. If the packet is an untagged packet, the packet will be matched against profiles on all IGMP Multicast VLANs. If it matches profiles on one of the IGMP Multicast VLAN, the packet will be associated with this VLAN. If it does not match profiles on any VLANs, then the packet is an umatched packet. If the packet is an unmatched packet, it will not be processed by the IGMP Multicast VLAN. Instead, it will be processed based on the forwarding mode for unmatched packets and the classified VLAN of this packet.  **Note:** The same profile can not be overlapped in different IGMP Multicast VLANs if these IGMP Multicast VLANs have an overlapping portlist. Multiple profiles can be added to a multicast VLAN.
Parameters	*<vlan_name 32>* – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. *add* – Used to associate a profile to a multicast VLAN. *delete* – Used to remove a profile from a multicast VLAN. *<profile_name 32>* – The name of the IPv4 multicast VLAN group profile to be associated the specified multicast VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add a group to an IGMP Multicast VLAN:

```
DGS-3700-12:5#config igmp_snooping multicast_vlan_group mv1 add profile_name RG
Command: config igmp_snooping multicast_vlan_group mv1 add profile_name RG

Success.

DGS-3700-12:5#
```

show igmp_snooping multicast_vlan_group

Purpose	Used to display the multicast groups configured for the specified IGMP Multicast VLAN.
Syntax	**show igmp_snooping multicast_vlan_group {< vlan_name 32> }**
Description	This command is used to display the multicast groups configured for the specified IGMP Multicast VLAN.
Parameters	*vlan_name* – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters.
Restrictions	None.

Example usage:

To display the multicast groups configured for an IGMP Multicast VLAN.

```
DGS-3700-12:5#show igmp_snooping multicast_vlan_group RG
Command: show igmp_snooping multicast_vlan_group RG

VLAN Name             VLAN ID  Multicast Group Profiles
--------------------  -------  --------------------------------
RG                     11

DGS-3700-12:5#
```

delete igmp_snooping multicast_vlan

Purpose	Used to delete an IGMP Muticast VLAN.
Syntax	**delete igmp_snooping multicast_vlan <vlan_name 32>**
Description	This command allows you to delete an IGMP Multicast VLAN.
Parameters	*vlan_name* – The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an IGMP Multicast VLAN:

```
DGS-3700-12:5#delete igmp_snooping multicast_vlan v1
Command: delete igmp_snooping multicast_vlan v1

Success.

DGS-3700-12:5#
```

enable/disable igmp_snooping multicast_vlan

Purpose	Used to enable/disable the IGMP Multicast VLAN function.

enable/disable igmp_snooping multicast_vlan

Syntax	**enable igmp_snooping multicast_vlan** **disable igmp_snooping multicast_vlan**
Description	This command controls the IGMP Multicast VLAN function. The IGMP Multicast VLAN will take effect when igmp snooping multicast vlan is enabled. By default, the IGMP Multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable IGMP Multicast VLAN:

```
DGS-3700-12:5#enable igmp_snooping multicast_vlan
Command: enable igmp_snooping multicast_vlan

Success.

DGS-3700-12:5#
```

show igmp_snooping multicast_vlan

Purpose	Used to show the information of IGMP Multicast VLAN.
Syntax	**show igmp_snooping multicast_vlan {<vlan_name 32>}**
Description	This command allows you to show the information of IGMP Multicast VLAN.
Parameters	*<vlan_name>* – The name of the multicast VLAN to be shown.
Restrictions	None.

Example usage:

To display IGMP Multicast VLAN:

```
DGS-3700-12:5#show igmp_snooping multicast_vlan
Command: show igmp_snooping multicast_vlan

IGMP Multicast VLAN Global State    : Enabled

VLAN Name                : RG
VID                      : 11

Member(Untagged) Ports   : 4-5
Tagged Member Ports      :
Source Ports             :
Status                   : Enabled
Replace Source IP        : 0.0.0.0

Total Entry: 1

DGS-3700-12:5#
```

create igmp_snooping multicast_vlan_group_profile

Purpose	Used to create an IGMP Multicast VLAN group profile on the switch.

create igmp_snooping multicast_vlan_group_profile

Syntax	**create igmp_snooping multicast_vlan_group_profile <profile_name 1-32>**
Description	This command is used to create an IGMP Multicast VLAN group profile. The profile name cannot be used for IGMP snooping or MLD snooping.
Parameters	*<profile_name 32>* – Specifies the IPv4 multicast VLAN group profile name, max length is 32. If not specified, all IPv4 multicast VLAN group profiles will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an IGMP multicast VLAN group profile "p1":

```
DGS-3700-12:5#create igmp_snooping multicast_vlan_group_profile p1
Command: create igmp_snooping multicast_vlan_group_profile p1

Success.

DGS-3700-12:5#
```

config igmp_snooping multicast_vlan_group_profile

Purpose	Used to configure an IGMP Multicast VLAN group profile on the switch, to add or delete multicast address on the profile.
Syntax	**config igmp_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast_address_list>**
Description	This command configures an IGMP Multicast VLAN group profile on the switch, to add or delete multicast address for the profile.
Parameters	*<profile_name 32>* – Specifies the IGMP Multicast VLAN group profile name, max length is 32. *[add | delete]* – Add or delete IGMP Multicast address list to or from this multicast VLAN group profile *<mcast_address_list>* – Specifies the IGMP Multicast addresses to be configured. It can be continuous single multicast addresses, such as 225.1.1.1, 225.1.1.3, 225.1.1.8, or a multicast address range, such as 225.1.1.1-225.2.2.2, or both of them, such as 225.1.1.1, 225.1.1.18-225.1.1.20
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add 233.1.1.1 to 266.1.1.1 to IGMP multicast VLAN group profile "p1":

```
DGS-3700-12:5#config igmp_snooping multicast_vlan_group_profile p1 add 225.1.1.1-
226.1.1.1
Command: config igmp_snooping multicast_vlan_group_profile p1 add 225.1.1.1-
226.1.1.1

Success.

DGS-3700-12:5#
```

delete igmp_snooping multicast_vlan_group_profile

Purpose	Used to delete an IGMP Multicast VLAN group profile on the switch.
Syntax	**delete igmp_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> |all]**
Description	This command deletes an IGMP Multicast VLAN group profile on the switch.
Parameters	*<profile_name 32>* – Specifies the IGMP Multicast VLAN profile name, max length is 32. *all* – All IGMP Multicast VLAN group profiles will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the IGMP multicast VLAN group profile "p1":

```
DGS-3700-12:5#delete igmp_snooping multicast_vlan_group_profile profile_name p1
Command: delete igmp_snooping multicast_vlan_group_profile profile_name p1

Success.

DGS-3700-12:5#
```

show igmp_snooping multicast_vlan_group_profile

Purpose	Used to view an IGMP Multicast VLAN group profile on the switch.
Syntax	**show igmp_snooping multicast_vlan_group_profile {<profile_name 1-32>}**
Description	This command displays an IGMP Multicast VLAN group profile on the switch.
Parameters	*{<profile_name 32>}* – Specifies the IGMP Multicast VLAN profile name, max length is 32. If not specifies, all IGMP Multicast VLAN group profile will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the IGMP Multicast VLAN group profile "p1":

```
DGS-3700-12:5#show igmp_snooping multicast_vlan_group_profile p1
Command: show igmp_snooping multicast_vlan_group_profile p1

Profile Name                    Multicast Addresses
------------------------------- -------------------------------
p1                              225.1.1.1-226.1.1.1

DGS-3700-12:5#
```

config igmp_snooping multicast_vlan forward_unmatched

Purpose	Used to configure forwarding mode for IGMP Multicast VLAN unmatched packets.
Syntax	**config igmp_snooping multicast_vlan forward_unmatched [disable | enable]**
Description	When the switch receives an IGMP packet, it will match the packet against the multicast profile to determine the multicast VLAN to be associated with. If the packet does not match any profiles, the packet will be forwarded or dropped based on the the setting. By default, the packet will be dropped.
Parameters	*enable* – The unmatched packet will be flooded on the VLAN. *disable* – The unmatched packet will be dropped.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set unmatched packets to be flooded on the VLAN:

```
DGS-3700-12:5#config igmp_snooping multicast_vlan forward_unmatched enable
Command: config igmp_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3700-12:5#
```

33

MLD MULTICAST VLAN COMMANDS

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

Command	Parameters
create mld_snooping multicast_vlan	<vlan_name 32> <vlanid 2-4094>
config mld_snooping multicast_vlan	<vlan_name 32> {[add | delete] [member_port <portlist> | source_port <portlist> |tag_member_port <portlist>]| state [enable|disable] |replace_source_ip <ipv6addr>}(1)
create mld_snooping multicast_vlan_group_profile	<profile_name 1-32>
config mld_snooping multicast_vlan_group_profile	<profile_name 1-32> [add | delete] <mcastv6_address_list>
delete mld_snooping multicast_vlan_group_profile	[profile_name <profile_name 1-32> |all]
show mld_snooping multicast_vlan_group_profile	{<profile_name 1-32>}
config mld_snooping multicast_vlan_group	<vlan_name 32> [add | delete] profile_name <profile_name 1-32>
show mld_snooping multicast_vlan_group	{< vlan_name 32> }
delete mld_snooping multicat_vlan	<vlan_name 32>
enable mld_snooping multicast_vlan	
disable mld_snooping multicast_vlan	
show mld_snooping multicast_vlan	{<vlan_name 32>}
config mld_snooping multicast_vlan forward_unmatched	[disable | enable]

Each command is listed, in detail, in the following sections.

create mld_snooping multicast_vlan

Purpose	Used to create an MLD multicast VLAN
Syntax	**create mld_snooping multicast_vlan <vlan_name 32> <vlanid 2-4094>.**
Description	This command is used to create a MLD multicast_vlan. Multiple multicast VLANs can be configured. The MLD multicast VLAN being created can not exist in the 1Q VLAN database. Multiple MLD multicast VLANs can be created. The MLD Multicast VLAN snooping function co-exists with the 1Q VLAN snooping function.
Parameters	*<vlan_name>* – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. *vlanid* – The VLAN ID of the multicast VLAN to be create. The range is 2-4094.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create MLD multicast VLAN mv1:

```
DGS-3700-12:5#create mld_snoop multicast_vlan mv1 2
Command: create mld_snooping multicast_vlan mv1 2

Success.

DGS-3700-12:5#
```

config mld_snooping multicast_vlan

Purpose	Used to configure the parameter of the specific MLD multicast VLAN.
Syntax	**config mld_snooping multicast_vlan <vlan_name 32> {[add|delete] [member_port <portlist>| tag_member_port <portlist> | source_port <portlist>] | state [enable | disable] | replace_source_ip <ipv6addr>}(1)**
Description	This command allows you to add member ports, add tag_member ports and add source ports to the port list. The member port will automatically become the untagged member of the MLD multicast VLAN, the tag_member_port and the source port will automatically become the tagged member of the MLD multicast VLAN. To change the port-list, the new port-list will replace the previous port-list if add or delete is not specified. The member port list and source port list can not overlap. However, the member port of one MLD multicast VLAN can overlap with another MLD multicast VLAN. The MLD multicast VLAN must be created first before configuration.
Parameters	*<vlan_name>* – The name of the VLAN to be created. Each multicast VLAN is given a name that can be up to 32 characters. *Member_port* – A range of member ports to add to the multicast VLAN. They will become the untagged member port of the MLD multicast VLAN. *tag_member_port* – Specifies the tagged member port of the MLD multicast VLAN. *source_port* – A range of source ports to add to the multicast VLAN. State – enable or disable multicast VLAN for the chosen VLAN. *replace_source_ip* – With the MLD snooping function, the MLD report packet sent by the host will be forwarded to the source port. Before the forwarding of the packet, the source IP address in the join packet needs to be replaced by this IPv6 address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config MLD multicast VLAN mv1:

```
DGS-3700-12:5#config mld_snooping multicast_vlan mv1 add member_port
1,3 state enable
Command: config mld_snooping multicast_vlan mv1 add member_port 1,3
state enable

Success.

DGS-3700-12:5#
```

create mld_snooping multicast_vlan_group_profile

Purpose	Used to create an MLD multicast VLAN group profile on the switch.
Syntax	**create mld_snooping multicast_vlan_group_profile <profile_name 1-32>**
Description	This command is used to create an MLD multicast VLAN group profile. The profile name used for mld snooping must be unique.
Parameters	*<profile_name 32>* – Specifies the MLD multicast VLAN group profile name, max length is 32
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an MLD multicast VLAN group profile "g1":

```
DGS-3700-12:5#create mld_snooping multicast_vlan_group_profile g1
Command: create mld_snooping multicast_vlan_group_profile g1

Success.

DGS-3700-12:5#
```

config mld_snooping multicast_vlan_group_profile

Purpose	Used to configure an MLD multicast VLAN group profile on the switch, to add or delete multicast address for the profile.
Syntax	**config mld_snooping multicast_vlan_group_profile <profile_name 1-32> [add | delete] <mcast v6_address_list>**
Description	This command configures an MLD multicast VLAN group profile on the switch, and can add or delete multicast addresses for the profile.
Parameters	*<profile_name 32>* – Specifies the MLD multicast VLAN group profile name, max length is 32. *[add | delete]* – Add or delete MLD multicast address list to or from this multicast VLAN group profile *<mcastv6_address_list>* – Specifies the MLD multicast addresses to be configured. It can be a continuous single multicast addresses, such as FF12::1, FF12::3, FF12::8, or a multicast address range, such as FF12::1- FF12::12, or both of them, such as FF12::1, FF12::18-FF12::20.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add 225.1.1.1 to 226.1.1.1 to MLD multicast VLAN group profile "g1":

```
DGS-3700-12:5#config mld_snooping multicast_vlan_group_profile g1
add FF12::1-FF12::2
Command: config mld_snooping multicast_vlan_group_profile g1 add
FF12::1-FF12::2

Success.

DGS-3700-12:5#
```

delete mld_snooping multicast_vlan_group_profile

Purpose	Used to delete an MLD multicast VLAN group profile on the switch.
Syntax	**delete mld_snooping multicast_vlan_group_profile [profile_name <profile_name 1-32> |all]**
Description	This command deletes an MLD multicast VLAN group profile on the switch.
Parameters	*<profile_name 32>* – Specifies the MLD multicast VLAN profile name, max length is 32. *all* – All MLD multicast VLAN group profile will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the MLD multicast VLAN group profile "g1":

```
DGS-3700-12:5#delete mld_snooping multicast_vlan_group_profile profile_name g1
Command: delete mld_snooping multicast_vlan_group_profile profile_name g1

Success.

DGS-3700-12:5#
```

show mld_snooping multicast_vlan_group_profile

Purpose	Used to view an MLD multicast VLAN group profile on the switch.
Syntax	**show mld_snooping multicast_vlan_group_profile {<profile_name 1-32>}**
Description	This command displays an MLD multicast VLAN group profile on the switch.
Parameters	*{<profile_name 32>}* – Specifies the MLD multicast VLAN profile name, max length is 32. If not specified, all MLD multicast VLAN group profiles will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To display the MLD multicast VLAN group profile:

```
DGS-3700-12:5#show mld_snooping multicast_vlan_group_profile
Command: show mld_snooping multicast_vlan_group_profile

Profile Name                    Multicast Addresses
------------------------------- -------------------------------
g1                              FF12::1-FF12::2


Total Entry: 1


DGS-3700-12:5#
```

config mld_snooping multicast_vlan multicast_group

Purpose	Used to configure the multicast group which will be learned with the specific MLD multicast VLAN.
Syntax	**config mld_snooping multicast_vlan_group <vlan_name 32> [add | delete] profile_name <profile_name 1-32>**
Description	When a MLD packet is received, first, it will be checked whether to be processed by MLD snooping. If MLD snooping for the classified VLAN of this MLD packet is enabled, it will be processed, based on the MLD snooping function. If the MLD snooping for the classified VLAN of this MLD packet is disabled, then it will check whether to be processed by the MLD multicast VLAN function. There are some cases when an MLD packet can be processed by the MLD multicast VLAN. If there are no profiles system wide, and there is only one MLD multicast VLAN, then this MLD packet will be associated with only this MLD multicast VLAN. However if the packet is a tagged packet, the packet will be matched against the profile on this VLAN. If matched, the packet will be associated with this VLAN. Otherwise, the packet is an unmatched packet. Otherwise if the packet is an untagged packet, the packet will be matched against profiles on all MLD multicast VLANs. If it matches profiles on one of the MLD multicast VLANs, the packets will be associated with this VLAN. If it does not match profiles on any VLANs, then the packet is an umatched packet. If the packet is an unmatched packet, it will not be processed by the MLD Multicast VLAN. Instead, it will be processed based on the forwarding mode for unmatched packets and the classified VLAN of this packet. **Note:** The same profile can not be overlapped in different multicast VLANs if these multicast VLANs have an overlapping portlist. Multiple profiles can be added to a multicast VLAN.
Parameters	*<vlan_name 32>* – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. *add* – Used to associate a profile to a multicast VLAN. *delete* – Used to de-associate a profile from a multicast VLAN. *<profile_name 32>* – The name of the MLD multicast VLAN group profile to be associated or de- associated to the specified multicast VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To associate an MLD multicast VLAN group profile "g1" to MLD multicast VLAN "mv1":

```
DGS-3700-12:5#config mld_snooping multicast_vlan_group mv1 add profile_name g1
Command: config mld_snooping multicast_vlan_group mv1 add profile_name g1

Success.

DGS-3700-12:5#
```

show mld_snooping multicast_vlan_group

Purpose	Used to display the multicast groups configured for the specified MLD multicast VLAN.
Syntax	**show mld_snooping multicast_vlan_group {< vlan_name 32> }**
Description	This command is used to display the multicast groups configured for the specified MLD multicast VLAN.
Parameters	*vlan_name* – The name of the multicast VLAN to be configured, each multicast VLAN is given a name that can be up to 32 characters. If not specified, all IPv6 multicast VLAN groups will be displayed.
Restrictions	None.

Example usage:

To display the multicast groups configured for an MLD multicast VLAN.

```
DGS-3700-12:5#show mld_snooping multicast_vlan_group
Command: show mld_snooping multicast_vlan_group

VLAN Name                       VLAN ID  Multicast Group Profiles
------------------------------  -------  ------------------------
mv1                             2         g1

DGS-3700-12:5#
```

delete mld_snooping multicast_vlan

Purpose	Used to delete an MLD muticast VLAN.
Syntax	**delete mld_snooping multicat_vlan <vlan_name 32>**
Description	This command is used to delete an MLD multicast VLAN.
Parameters	*vlan_name* – The name of the multicast VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete an MLD multicast VLAN:

```
DGS-3700-12:5#delete mld_snooping multicast_vlan mv1
Command: delete mld_snooping multicast_vlan mv1

Success.

DGS-3700-12:5#
```

enable/disable mld_snooping multicast_vlan

Purpose	Used to enable/disable the MLD Multicast VLAN function.
Syntax	**enable mld_snooping multicast_vlan** **disable mld_snooping multicast_vlan**
Description	This command controls the MLD Multicast VLAN function. The MLD Multicast VLAN will take effect when MLD snooping multicast VLAN is enabled. By default, the MLD Multicast VLAN is in a disabled state.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MLD Multicast VLAN:

```
DGS-3700-12:5#enable mld_snooping multicast_vlan
Command: enable mld_snooping multicast_vlan

Success.

DGS-3700-12:5#
```

show mld_snooping multicast_vlan

Purpose	Used to show the information of MLD multicast VLAN.
Syntax	**show mld_snooping multicast_vlan {<vlan_name 32>}**
Description	This command is used to show the information of an MLD multicast VLAN.
Parameters	*<vlan_name>* – The name of the multicast VLAN to be shown. If not specified, all MLD multicast VLANs will be displayed.
Restrictions	None.

Example usage:

To show MLD multicast VLAN:

```
DGS-3700-12:5#show mld_snooping multicast_vlan mv1
Command: show mld_snooping multicast_vlan mv1

MLD Multicast VLAN Global State    : Disabled

VLAN Name                : mv1
VID                      : 23

Member(Untagged) Ports   :
Tagged Member Ports      :
Source Ports             :
Status                   : Disabled
Replace Source IP        : ::

Total Entry: 1

DGS-3700-12:5#
```

config mld_snooping multicast_vlan forward_unmatched

Purpose	Used to configure forwarding mode for MLD Multicast VLAN unmatched packet.
Syntax	**config mld_snooping multicast_vlan forward_unmatched [disable | enable]**
Description	When the switch receives an MLD packet, it will match the packet against the multicast profile to determine the MLD multicast VLAN to be associated with. If the packet does not match any profiles, the packet will be forwarded or dropped based on the setting. By default, the packet will be dropped.
Parameters	*enable* – The unmatched packet will be flooded on the VLAN. *disable* – The unmatched packet will be dropped.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set unmatched packet to be flooded on the VLAN:

```
DGS-3700-12:5#config mld_snooping multicast_vlan forward_unmatched enable
Command: config mld_snooping multicast_vlan forward_unmatched enable

Success.

DGS-3700-12:5#
```

34

MLD SNOOPING COMMAND LIST

The MLD Snooping Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config mld_snooping	[vlan <vlan_name 32> | vlanid <vidlist> |all] { state [enable|disable] | fast_done [enable|disable] | report_suppression [enable | disable]}(1)
config mld_snooping querier	[vlan <vlan_name 32> | vlanid <vidlist> |all] { query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> | state [enable|disable] |version <value 1-2>}(1)
config mld_snooping mrouter_ports	[vlan <vlan_name 32> | vlanid <vidlist>] [add|delete] <portlist>
config mld_snooping mrouter_ports_forbidden	[vlan <vlan_name 32> | vlanid <vidlist>] [add|delete]<portlist>
enable mld_snooping	
disable mld_snooping	
show mld_snooping	{[vlan <vlan_name 32> | vlanid <vidlist>]}
show mld_snooping group	{[vlan <vlan_name 32> | vlanid <vidlist> | ports <portlist>] {<ipv6addr>}} {data_driven}
show mld_snooping mrouter_ports	[vlan <vlan_name 32> | vlanid <vidlist> |all] { [static|dynamic|forbidden]}
show mld_snooping rate_limit	[ports <portlist>|vlanid <vlanid_list>]
config mld_snooping rate_limit	[ports <portlist>|vlanid <vlanid_list>] [<value 1-1000> | no_limit]
show mld_snooping forwarding	{[vlan <vlan_name 32> | vlanid <vlanid_list>]}
show mld_snooping static_group	{[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipv6addr >}
create mld_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] < ipv6addr >
delete mld_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] < ipv6addr >
config mld_snooping static_group	[vlan <vlan_name 32> | vlanid <vlanid_list>] < ipv6addr > [add | delete] <portlist>
show mld_snooping statistic counter	[vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]
clear mld_snooping statistic counter	
config mld_snooping data_driven_learning max_learned_entry	<value 1-1024>
config mld_snooping data_driven_learning	[all | vlan_name <vlan_name> | vlanid <vlanid_list>] { state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)
clear mld_snooping data_driven_group	[all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipv6addr >| all]]

Each command is listed, in detail, in the following sections.

config mld_snooping

Purpose	Used to configure MLD snooping on the switch.
Syntax	**config mld_snooping [vlan <vlan_name 32> | vlanid <vidlist> |all] { state [enable|disable] | fast_done [enable|disable] | report_suppression [enable | disable]}(1)**
Description	This command is used to configure MLD snooping on the switch. If the MLD version is configured with a lower version, the higher version's MLD Report/Leave messages will be ignored.
Parameters	*vlan_name* – The name of the VLAN for which MLD snooping is to be configured. *vidlist* – The VIDs of the VLAN for which MLD snooping is to be configured. *all* – Specifies that all VLANs configured on the switch will be configured. *state* – Allows the user to enable or disable the MLD snooping function for the chosed VLAN. *fast_done* – enable or disable MLD snooping fast_done function.If enable, the membership is immediately removed when the system receive the MLD done message. *report suppression* – Enables or Disables MLD snooping report suppression function. If enabled, multiple MLD reports are done for a specific (S,G) and will be intregrated into one report only before sending to the router port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MLD snooping to the default vlan with noted_timeout 250 sec and state enable:

```
DGS-3700-12:5#config mld_snooping vlan default state enable
Command: config mld_snooping vlan default state enable

Success.

DGS-3700-12:5#
```

config mld_snooping querier

Purpose	Used to configure the timers and the attributes of the MLD snooping.querier.
Syntax	**config mld_snooping querier [vlan <vlan_name 32> | vlanid <vidlist> |all] { query_interval <sec 1-65535> | max_response_time <sec 1-25> | robustness_variable <value 1-255> | last_listener_query_interval <sec 1-25> | state [enable|disable] |version <value 1-2>}(1)**
Description	This command is used to configure the timer in seconds between general query transmissions, the maximum time in seconds to wait for reports from listeners, and the permitted packet loss that guarantees MLD snooping.
Parameters	*vlan_name* – The name of the VLAN for which MLD snooping is to be configured. *vidlist* – The VIDs of the VLAN for which MLD snooping querier is to be configured. *query_interval* – Specifies the amount of time in seconds between general query transmissions. The default setting is *125* seconds. *max_reponse_time* – The maximum time in seconds to wait for reports from listeners. The default setting is *10* seconds. *robustness_variable* – Provides fine-tuning to allow for expected packet loss on a subnet. The value of the robustness variable is used in calculating the following MLD message intervals: • *group listener interval* – Amount of time that must pass before a multicast router decides there are no more listeners of a group on a network. This interval is calculated as follows: (robustness variable * query interval) + (1 * query response interval). • *other querier present interval* – Amount of time that must pass before a multicast router decides that there is no longer another multicast router that is the querier. This interval is calculated as follows: (robustness variable * query interval) + (0.5 * query response interval). • *last listener query count* – Number of group-specific queries sent before the router assumes there are no local listeners of a group. The default number is the value of the robustness variable. • By default, the robustness variable is set to *2*. You might want to increase this value if you expect a subnet to be lossy. *last_listener_query_interval* – The maximum amount of time between group-specific query messages, including those sent in response to done-group messages. You might lower this interval to reduce the amount of time it takes a router to detect the loss of the last listener of a group. *state* – Allows you to enable or disable the MLD snooping function for the chosen VLAN. *version* – The version of MLD Query sent by the switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MLD snooping querier query interval to 125 secs and state enable:

```
DGS-3700-12:5#config mld_snooping querier vlan default query_interval 125 state enable
Command: config mld_snooping querier vlan default query_interval 125 state enable

Success.

DGS-3700-12:5#
```

config mld_snooping mrouter_ports

Purpose	Used to configure ports as router ports.
Syntax	**config mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vidlist>] [add|delete] <portlist>**
Description	This command is used to designate a range of ports as being connected to multicast-enabled routers. This will ensure that all packets with such a router as its destination will reach the multicast-enabled router – regardless of protocol, etc.
Parameters	*vlan_name* – The name of the VLAN for which MLD snooping is to be configured. *vlanid list* – The VIDs of the VLAN for which MLD snooping is to be configured. *add* | *delete* – Specifies to add or delete the router ports. *portlist* – Specifies a range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up port range 1-10 to be static router ports:

```
DGS-3700-12:5#config mld_snooping mrouter_ports vlan default add 1-10
Command: config mld_snooping mrouter_ports vlan default add 1-10

Success.

DGS-3700-12:5#
```

config mld_snooping mrouter_ports_forbidden

Purpose	Used to configure ports as forbidden router ports.
Syntax	**config mld_snooping mrouter_ports_forbidden [vlan <vlan_name 32> | vlanid <vidlist>] [add|delete] <portlist>**
Description	This command is used to designate a range of ports as being not connected to multicast-enabled routers. This ensures that the forbidden router port will not propagate routing packets out.
Parameters	*vlan_name* – The name of the VLAN for which MLD snooping is to be configured. *vlanid list* – The VIDs of the VLAN for which MLD snooping is to be configured. *add* | *delete* – Specifies to add or delete the router ports. *portlist* – Specifies a range of ports to be configured as forbidden router ports.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set up port range 1-10 to static router ports:

```
DGS-3700-12:5#config mld_snooping mrouter_ports_forbidden vlan default add 1-10
Command: config mld_snooping mrouter_ports_forbidden vlan default add 1-10

Success.

DGS-3700-12:5#
```

enable mld_snooping

Purpose	Used to enable MLD snooping on the switch.
Syntax	**enable mld_snooping**
Description	This command is used to enable MLD snooping on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MLD snooping on the switch:

```
DGS-3700-12:5#enable mld_snooping
Command: enable mld_snooping

Success.

DGS-3700-12:5#
```

disable mld_snooping

Purpose	Used to disable MLD snooping on the switch.
Syntax	**disable mld_snooping**
Description	This command is used to disable MLD snooping on the switch. Disabling MLD snooping allows all MLD and IPv6 multicast traffic to flood within a given IPv6 interface.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable MLD snooping on the switch:

```
DGS-3700-12:5#disable mld_snooping
Command: disable mld_snooping

Success.

DGS-3700-12:5#
```

show mld_snooping

Purpose	Used to the current status of MLD snooping on the switch.
Syntax	**show mld_snooping {[vlan <vlan_name 32> | vlanid <vidlist>]}**
Description	This command is used to display the current MLD snooping configuration on the switch.
Parameters	*vlan_name* – The name of the VLAN for which you want to view the MLD snooping configuration. *vlanid list* – The VIDs of the VLAN for which you want to view the MLD snooping configuration. If no parameter specified, the system will display all current MLD snooping configurations.
Restrictions	None.

Example usage:

To show MLD snooping on the switch:

```
DGS-3700-12:5#show mld_snooping
Command: show mld_snooping

MLD Snooping Global State               : Disabled
Data Driven Learning Max Entries        : 128

 VLAN Name                      : default
 Query Interval                 : 125
 Max Response Time              : 10
 Robustness Value               : 2
 Last Listener Query Interval   : 1
 Querier State                  : Disable
 Querier Role                   : Non-Querier
 Querier IP                     :
 Querier Expiry Time            : 0 secs
 State                          : Disable
 Fast Done                      : Disable
 Report Suppression             : Enable
 Rate Limit                     : No Limitation
 Version                        : 2
 Data Driven Learning State     : Enable
 Data Driven Learning Aged Out  : Disable
 Data Driven Group Expiry Time  : 260

Total Entries: 1
DGS-3700-12:5#
```

show mld_snooping group

Purpose	Used to display the current MLD snooping group configuration on the switch.
Syntax	**show mld_snooping group {[vlan <vlan_name 32> | vlanid <vidlist> | ports <portlist>] {<ipv6addr>}} {data_driven}**
Description	This command is used to display the current MLD snooping group configuration on the switch.
Parameters	*vlan_name* – The name of the VLAN for which you want to view the MLD snooping configuration. *vlanid_list* – The VIDs of the VLAN for which you want to view the MLD snooping group configuration. *portlist* – The list of the ports for which you want to view the MLD snooping group configuration. *<ipv6addr>* – To view the information of this specified group. *data_driven* – To view the groups learnt by data driven only. If no parameter is specified, the system will display all current MLD snooping groups.
Restrictions	None.

Example usage:

To show MLD snooping group on the switch:

```
DGS-3700-12:5#show mld_snooping group
Command: show mld_snooping group

Source/Group     : 2001::2/FF1E::1
VLAN Name/VID    : default/1
Member Ports     : 12
UP Time          : 2
Expiry Time      : 258
Filter Mode      : INCLUDE

Total Entries : 1

DGS-3700-12:5#
```

show mld_snooping mrouter_ports

Purpose	Used to display the currently configured router ports on the switch.
Syntax	**show mld_snooping mrouter_ports [vlan <vlan_name 32> | vlanid <vidlist> |all] {[static|dynamic|forbidden]}**
Description	This command is used to display the currently configured router ports on the switch.
Parameters	*vlan_name* – The name of the VLAN for which you want to view the MLD snooping configuration. *vid list* – The VIDs of the VLAN for which you want to view the MLD snooping configuration. *all* – All the MLD router ports will be displayed. *static* – Displays router ports that have been statically configured. *dynamic* – Displays router ports that have been dynamically configured. *forbidden* – Displays forbidden router ports that have been statically configured. If no parameter specified, the system will display all currently configured router ports on the switch.
Restrictions	None.

Example usage:

To display the router ports on the switch:

```
DGS-3700-12:5#show mld_snooping mrouter_ports all
Command: show mld_snooping mrouter_ports all

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

 Total Entries: 1

DGS-3700-12:5#
```

show mld_snooping rate_limit

Purpose	Used to show rate limitation.
Syntax	**show mld_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>]**
Description	This command shows the rate of MLD control packets that are allowed per port or VLAN.
Parameters	*<portlist>* – Specifies a port or range of ports that will be displayed. *<vlanid_list>* – Specifies a VLAN or range of VLANs that will be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To show rate limitation:

```
DGS-3700-12:5#show mld_snooping rate_limit ports 1
Command: show mld_snooping rate_limit ports 1

 Port      Rate Limitation
 --------  ---------------
 1         No Limitation

Total Entries: 1

DGS-3700-12:5#
```

config mld_snooping rate_limit

Purpose	Used to show MLD snooping rate limitation.
Syntax	**config mld_snooping rate_limit [ports <portlist>|vlanid <vlanid_list>] [<value 1-1000> | no_limit]**
Description	This command configures the rate of MLD control packets that are allowed per port or VLAN.
Parameters	*<portlist>* – Specifies a port or range of ports that will be configured. *<vlanid_list>* – Specifies a VLAN or range of VLANs that will be configured. *<value 1-1000>* – Specifies the rate of MLD control packets that the switch can process on a specific port. The rate is specified in packets per second. The packet that exceeds the limited rate will be dropped. The default setting is no_limit. *no_limit* – Allows user to configure the rate limitation to no limit.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure rate limitation:

```
DGS-3700-12:5#config mld_snooping rate_limit ports 1 100
Command: config mld_snooping rate_limit ports 1 100

Success.

DGS-3700-12:5#
```

show mld_snooping forwarding

Purpose	Used to display the current MLD snooping forwarding information on the Switch.
Syntax	**show mld_snooping forwarding {[vlan <vlan_name 32> | vlanid <vlanid_list>]}**
Description	This command will display the current MLD forwarding information on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view MLD snooping forwarding information. If not specified, all VLAN's MLD snooping forwarding information will be displayed. *<vlanid_list>* – The list of the VLAN IDs for which to view MLD snooping forwarding information. If not specified, all VLAN's MLD snooping forwarding information will be displayed.
Restrictions	None.

Example usage:

To view the current MLD snooping forwarding information:

```
DGS-3700-12:5#show mld_snooping forwarding
Command: show mld_snooping forwarding

 VLAN Name                      : default
 Source IP                      : *
 Multicast Group                : FF12::1
 Port Member                    : 3

 VLAN Name                      : default
 Source IP                      : *
 Multicast Group                : FF12::2
 Port Member                    : 3

 Total Entries : 2

DGS-3700-12:5#
```

show mld_snooping static_group

Purpose	Used to display the current MLD snooping static group information on the Switch.
Syntax	**show mld_snooping static_group {[vlan <vlan_name 32>| vlanid <vlanid_list>] < ipv6addr >}**
Description	This command is used to display the current MLD snooping static group information on the Switch.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view MLD snooping static group information, if not specified, all static group will be displayed. *<vlanid_list>* – The list of the VLAN IDs for which to view MLD snooping static group information, if not specified, all static group will be displayed. *< ipv6addr >* – The static group IPv6 address for which to view MLD snooping static group information.
Restrictions	None.

Example usage:

To view the current MLD snooping static group information:

```
DGS-3700-12:5#show mld_snooping static_group
Command: show mld_snooping static_group

VLAN ID/Name                IP Address           Static Member Ports
--------------------------  -------------------  ---------------
1   /default                FF12::1               3
1   /default                FF12::2               3

 Total Entries : 2


DGS-3700-12:5#
```

create mld_snooping static_group

Purpose	Used to display the current MLD snooping static group information on the Switch.
Syntax	**create mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr>**
Description	This command is used to create a mld snooping static group. Member ports can be added to the static group. The static member and the dynamic member port form the member ports of a group. The static group will only take effect when MLD snooping is enabled on the VLAN. For those static member ports, the device needs to emulate the MLD protocol operation to the querier, and forward the traffic destined to the multicast group to the member ports. For a layer 3 device, the device is also responsible to route the packet destined for this specific group to static member ports. The static member port will only affect V1 MLD operation. The Reserved IP multicast address FF0E::X must be excluded from the configured group. The VLAN must be created first before a static group can be created.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to create MLD snooping static group information. *<vlanid_list>* – The list of the VLAN IDs for which to create MLD snooping static group information. *< ipv6addr >* – The static group IPv6 address for which to create MLD snooping static group information.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a static group FF12::1 for VID 1:

```
DGS-3700-12:5#create mld_snooping static_group vlanid 1 FF12::1
Command: create mld_snooping static_group vlanid 1 FF12::1

Success.

DGS-3700-12:5#
```

delete mld_snooping static_group

Purpose	Used to delete the current MLD snooping static group on the Switch.
Syntax	**delete mld_snooping static_group [vlan <vlan_name 32> | vlanid < *vlanid_list* >] <ipv6addr>**
Description	This command is used to delete an MLD snooping static group will not affect the MLD snooping dynamic member ports of a group.
Parameters	*<vlan_name 32>* – The name of the VLAN for which MLD snooping static group information will be deleted. *<vlanid_list>* – The list of the VLAN IDs for which MLD snooping static group information will be deleted. < *ipv6addr* > – The static group IPv6 address for which MLD snooping static group information will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a static group FF12::1 on VID 1:

```
DGS-3700-12:5#delete mld_snooping static_group vlanid 1  FF12::1
Command: delete mld_snooping static_group vlanid 1  FF12::1

Success.

DGS-3700-12:5#
```

config mld_snooping static_group

Purpose	Used to configure the current MLD snooping static group on the Switch.
Syntax	**config mld_snooping static_group [vlan <vlan_name 32> | vlanid <vlanid_list>] <ipv6addr> [add | delete] <portlist>**
Description	This command is used to add or delete ports to/from the given static group.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to configure MLD snooping static group information. *<vlanid_list>* – The list of the VLAN IDs for which to configure MLD snooping static group information. < *ipv6addr* > – The static group IPv6 address for which to configure MLD snooping static group information. *[add* | *delete] <portlist>* – Portlist to add or delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add port 5 to static group FF12::1 on VID 1:

```
DGS-3700-12:5#config mld_snooping static_group vlanid 1  FF12::1 add 5
Command: config mld_snooping static_group vlanid 1  FF12::1 add 5

Success.

DGS-3700-12:5#
```

show mld_snooping statistic counter	
Purpose	Used to view the current MLD snooping statistic on the Switch.
Syntax	**show mld_snooping statistic counter [vlan <vlan_name 32> | vlanid <vlanid_list> | ports <portlist>]**
Description	This command is used to view this information, MLD snooping must be enabled first.
Parameters	*<vlan_name 32>* – The name of the VLAN for which to view MLD snooping statistic counter. *<vlanid_list>* – The list of the VLAN ID for which to view MLD snooping statistic counter. *<portlist>* – The list of the ports for which to view MLD snooping statistic counter.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To view MLD snooping statistic on VID 1:

```
DGS-3700-12:5#show mld_snooping statistic counter vlanid 1
Command: show mld_snooping statistic counter vlanid 1


VLAN Name         : default
-------------------------------------------------
Group Number      : 0

Receive Statistics
    Query
      MLD v1 Query                    : 0
      MLD v2 Query                    : 0
      Total                           : 0
      Dropped By Rate Limitation      : 0
      Dropped By Multicast VLAN       : 0

    Report & Done
      MLD v1 Report                   : 0
      MLD v2 Report                   : 0
      MLD v1 Done                     : 0
      Total                           : 0
      Dropped By Rate Limitation      : 0
      Dropped By Max Group Limitation : 0
      Dropped By Group Filter         : 0
      Dropped By Multicast VLAN       : 0

Transmit Statistics
    Query
      MLD v1 Query                    : 0
      MLD v2 Query                    : 0
      Total                           : 0

    Report & Done
      MLD v1 Report                   : 0
      MLD v2 Report                   : 0
      MLD v1 Done                     : 0
      Total                           : 0

 Total Entries : 1


DGS-3700-12:5#
```

clear mld_snooping statistic counter

Purpose	Used to clear the current MLD snooping statistic on the Switch.
Syntax	**clear mld_snooping statistic counter**
Description	This command is used to clear all MLD snooping statistic counters.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear MLD snooping statistic counter:

```
DGS-3700-12:5#clear mld_snooping statistic counter
Command: clear mld_snooping statistic counter

Success.

DGS-3700-12:5#
```

config mld_snooping data_driven_learning max_learned_entry

Purpose	Used to configure the max number of groups that can be learnt by data driven.
Syntax	**config mld_snooping data_driven_learning max_learned_entry <value 1-1024>**
Description	This command is used to configure the maximum number of groups that can be learnt by data driven. When the table is full, the system will stop learning the new data-driven groups. Traffic for the new groups will be dropped.
Parameters	*<value 1-1024 >* – The max number of groups that can be learned by data driven.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the max number of groups that can be learned by data driven to 100:

```
DGS-3700-12:5#config mld_snooping data_driven_learning max_learned_entry 100

Command: config mld_snooping data_driven_learning max_learned_entry 100

Success.

DGS-3700-12:5#
```

config mld_snooping data_driven_learning

Purpose	Used to configure the data driven learing of a MLD snooping group.
Syntax	**config mld_snooping data_driven_learning [all | vlan_name <vlan_name> | vlanid <vlanid_list>] { state [enable | disable] | aged_out [enable | disable] | expiry_time <sec 1-65535>}(1)**
Description	This command is used to enable/disable the data driven learing of a MLD snooping group. When data-driven learning is enabled for the VLAN, and the switch receives the IP multicast traffic on this VLAN, a MLD snooping group will be created. That is, the learning of an entry is not activated by MLD membership registration, but activated by the traffic. For an ordinary MLD snooping entry, the MLD protocol will take care regarding the ageing out of the entry. For a data-driven entry, the entry can be specified not to be ageout or to be ageout by the aged timer. When the data driven learning is enabled, and data driven table is not full, the multicast filtering mode for all ports are ignored. That is, the multicast packets will be forwarded to router ports. If the data driven learning table is full, the multicast packets will be forwarded according to multicast filtering mode. **Note:** If a data-driven group is created and MLD member ports are learned later, the entry will become an ordinary MLD snooping entry. Therefore the ageing out mechanism will follow the ordinary MLD snooping entry.
Parameters	*all* – Configure all VLAN's MLD Snooping configuration. *vlan_name <vlan_name 32>* – The name of the VLAN for which MLD snooping data driven learning is to be configured. *vlanid <vlanid_list>* – The VID of the VLAN for which MLD snooping data driven learning is to be configured. *state [enable | disable]* – Allows users to enable or disable MLD snooping data driven learning for the specified VLAN. *aged_out [enable|disable]* – Allows users to enable or disable aged_out of MLD Snooping data driven learning for the specified VLAN. *expiry_time <sec 1-65535>* – Allows users to set the time that an MLD Snooping data driven learning group will expire for the specified VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable mld data driven learning on VLAN default:

```
DGS-3700-12:5#config mld_snooping data_driven_learning vlan_name default state enable
aged_out enable expiry_time 270
Command: config mld_snooping data_driven_learning vlan_name default state enable
aged_out enable expiry_time 270

Success.

DGS-3700-12:5#
```

clear mld_snooping data_driven_group

Purpose	Used to delete the MLD snooping group learnt by data driven.
Syntax	**clear mld_snooping data_driven_group [all | [vlan_name <vlan_name> | vlanid <vlanid_list>] [<ipaddr>| all]]**
Description	This command is used to delete the MLD snooping group learnt by data driven.
Parameters	*all* – Delete all groups learnt by data driven. *vlan_name* <*vlan_name 32*> – The name of the VLAN for which MLD snooping data driven learning group is to be deleted. *vlanid* <*vlanid_list*> – The VID of the VLAN for which MLD snooping data driven learning group is to be deleted. <*ipaddr*> – The group address for which MLD snooping data driven learning group is to be deleted on the specified VLAN. <*all*> – All groups learnt by data driven on the specified VLAN will be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete all groups learnt by data driven on VLAN default:

```
DGS-3700-12:5#clear mld_snooping data_driven_group vlan_name default all
Command: clear mld_snooping data_driven_group vlan_name default all

Success.

DGS-3700-12:5#
```

35

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	Parameters
config mirror port	<port> {[add | delete] source ports <portlist> [rx | tx | both]}
enable mirror	
disable mirror	
show mirror	

Each command is listed, in detail, in the following sections.

config mirror port

Purpose	Used to configure a mirror port – source port pair on the Switch. Traffic from any source port to a target port can be mirrored for real-time analysis. A logic analyzer or an RMON probe can then be attached to study the traffic crossing the source port in a completely obtrusive manner.
Syntax	**config mirror port <port> {[add | delete] source ports <portlist> [rx | tx | both]}**
Description	This command allows a range of ports to have all of their traffic also sent to a designated port, where a network sniffer or other device can monitor the network traffic. In addition, users can specify that only traffic received by or sent by one or both is mirrored to the Target port.
Parameters	*<port>* – This specifies the Target port (the port where mirrored packets will be received). The target port must be configured in the same VLAN and must be operating at the same speed as the source port. If the target port is operating at a lower speed, the source port will be forced to drop its operating speed to match that of the target port. *[add | delete]* – Specifies if the user wishes to add or delete ports to be mirrored that are specified in the *source ports* parameter. *source ports* – The port or ports being mirrored. This cannot include the Target port. *<portlist>* – This specifies a port or range of ports that will be mirrored. That is, the range of ports in which all traffic will be copied and sent to the Target port. *rx* – Allows the mirroring of only packets received by (flowing into) the port or ports in the port list. *tx* – Allows the mirroring of only packets sent to (flowing out of) the port or ports in the port list. *both* – Mirrors all the packets received or sent by the port or ports in the port list.
Restrictions	The Target port cannot be listed as a source port. Only Administrator and Operator-level users can issue this command.

Example usage:

To add the mirroring ports:

```
DGS-3700-12:5#config mirror port 1 add source ports 2-5 both
Command: config mirror port 1 add source ports 2-5 both

Success.

DGS-3700-12:5#
```

Example usage:

To delete the mirroring ports:

```
DGS-3700-12:5#config mirror port 1 delete source port 2-4
Command: config mirror 1 delete source 2-4

Success.

DGS-3700-12:5#
```

enable mirror

Purpose	Used to enable a previously entered port mirroring configuration.
Syntax	**enable mirror**
Description	This 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 and Operator-level users can issue this command.

Example usage:

To enable mirroring configurations:

```
DGS-3700-12:5#enable mirror
Command: enable mirror

Success.

DGS-3700-12:5#
```

disable mirror

Purpose	Used to disable a previously entered port mirroring configuration.
Syntax	**disable mirror**
Description	This 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 and Operator-level users can issue this command.

Example usage:

To disable mirroring configurations:

```
DGS-3700-12:5#disable mirror
Command: disable mirror

Success.

DGS-3700-12:5#
```

show mirror

Purpose	Used to show the current port mirroring configuration on the Switch.
Syntax	**show mirror**
Description	This command displays the current port mirroring configuration on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display mirroring configuration:

```
DGS-3700-12:5#show mirror
Command: show mirror

Current Settings
Mirror Status : Enabled
Target Port   : 1
Mirrored Port
           RX :
           TX : 5-7

DGS-3700-12:5#
```

36

LOOP-BACK DETECTION COMMANDS

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

Command	Parameters
config loopdetect	{recover_timer [<value 0>| <value 60-1000000>] | interval <1-32767> | mode [port-based | vlan-based]}(1)
config loopdetect ports	[<portlist> | all] state [enabled|disabled]
enable loopdetect	
disable loopdetect	
show loopdetect	
show loopdetect ports	[all |<portlist>]
config loopdetect trap	[none | loop_detected | loop_cleared | both]

Each command is listed, in detail, in the following sections.

config loopdetect

Purpose	Used to configure loop-back detection on the switch.
Syntax	**config loopdetect {recover_timer [<value 0>| <value 60-1000000>] | interval <1-32767> | mode [port-based | vlan-based]}(1)**
Description	This command is used to configure loop-back detection on the switch.
Parameters	*recover_timer* – The time interval (in seconds) used by the Auto-Recovery mechanism to decide how long to check if the loop status is gone. The valid range is *60* to *1000000*. Zero is a special value which means to disable the auto-recovery mechanism. The default value is *60*. *interval* – The time interval (inseconds) at which the remote device transmits all the CTP packets to detect the loop-back event. The default value is *10*, with a valid range of *1* to *32767*. *mode* – In port-based mode, the port will be disabled during the loop detection. In vlan-based mode, the port can not process VLAN packets destined for ports involved in detecting the loop.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the recover time to 0, and interval to 20, and VLAN-based mode:

```
DGS-3700-12:5#config loopdetect recover_timer 0 interval 20 mode vlan-based
Command: config loopdetect recover_timer 0 interval 20 mode vlan-based

Success

DGS-3700-12:5#
```

config loopdetect ports

Purpose	Used to configure loop-back detection state of ports.
Syntax	**config loopdetect ports [<portlist> | all] | state [enabled | disabled]**
Description	This command is used to configure loop-back detection state of ports.
Parameters	*<portlist>* – Specifies a range of ports for the loop-back detection *state [enabled | disabled]* – Allows the loop-back detection to be disabled and enabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the loop-detect state to enable:

```
DGS-3700-12:5#config loopdetect ports 1-5 state enabled
Command: config loopdetect ports 1-5 state enabled

Success

DGS-3700-12:5#
```

enable loopdetect

Purpose	Used to globally enable loop-back detection on the switch.
Syntax	**enable loopdetect**
Description	This command is used to globally enable loop-back detection on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable loop-back detection on the switch:

```
DGS-3700-12:5#enable loopdetect
Command: enable loopdetect

Success

DGS-3700-12:5#
```

disable loopdetect

Purpose	Used to globally disable loop-back detection on the switch.
Syntax	**disable loopdetect**
Description	This command is used to globally disable loop-back detection on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable loop-back detection on the switch:

```
DGS-3700-12:5#disable loopdetect
Command: disable loopdetect

Success

DGS-3700-12:5#
```

show loopdetect

Purpose	Used to display the current loop-back detection settings on the switch.
Syntax	**show loopdetect**
Description	This command is used to display the current loop-back detection settings on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show loop-detect:

```
DGS-3700-12:5#show loopdetect
Command: show loopdetect

 LBD Global Settings
 ---------------------------
 LBD Status          : Disabled
 LBD Mode            : Port_based
 LBD Interval        : 10
 LBD Recover Time    : 60
 LBD Trap Status     : None

DGS-3700-12:5#
```

show loopdetect ports

Purpose	Used to display the current per-port loop-back detection settings on the switch.
Syntax	**show loopdetect ports [all | <portlist>]**
Description	This command is used to display the current per-port loop-back detection settings on the switch.
Parameters	*<portlist>* – Specifies a range of ports for the loop-back detection *all* – Specifies all ports for the loop-back detection.
Restrictions	None.

Example usage:

To show loop-detect ports:

```
DGS-3700-12:5#show loopdetect ports 1-3
Command: show loopdetect ports 1-3

Port   Loopdetect State    Loop Status
------ ----------------- ----------
1      Enabled             Normal
2      Enabled             Normal
3      Enabled             Normal

DGS-3700-12:5#
```

config loopdetect trap

Purpose	This command is used to config trap modes.
Syntax	**config loopdetect trap [none | loop_detected | loop_cleared | both]**
Description	The loop-detect trap is sent when the loop condition is detected. The loop-detect will be cleared when the trap is sent and the loop condition is cleared.
Parameters	*none* – Trap will not be sent for both cases. *loop_detected* – Trap is sent when the loop condition is detected. *loop_cleared* – Trap is sent when the loop condition is cleared. *both* – Trap will be sent for both cases.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config loop trap both:

```
DGS-3700-12:5#config loopdetect trap both
Command: config loopdetect trap both

Success.

DGS-3700-12:5#
```

37

MULTIPLE SPANNING TREE PROTOCOL (MSTP) COMMANDS

This Switch supports three versions of the Spanning Tree Protocol: 802.1D-2004 STP-compatible, 802.1D-2004 Rapid STP and 802.1Q-2005 MSTP. Multiple Spanning Tree Protocol, or MSTP, is a standard defined by the IEEE community that allows multiple VLANs to be mapped to a single spanning tree instance, which will provide multiple pathways across the network. Therefore, these MSTP configurations will balance the traffic load, preventing wide scale disruptions when a single spanning tree instance fails. This will allow for faster convergences of new topologies for the failed instance. Frames designated for these VLANs will be processed quickly and completely throughout interconnected bridges utilizing either of the three spanning tree protocols (STP, RSTP or MSTP). This protocol will also tag BDPU packets so receiving devices can distinguish spanning tree instances, spanning tree regions and the VLANs associated with them. These instances will be classified by an *instance_id*. MSTP will connect multiple spanning trees with a Common and Internal Spanning Tree (CIST). The CIST will automatically determine each MSTP region, its maximum possible extent and will appear as one virtual bridge that runs a single spanning tree. Consequentially, frames assigned to different VLANs will follow different data routes within administratively established regions on the network, continuing to allow simple and full processing of frames, regardless of administrative errors in defining VLANs and their respective spanning trees. Each switch utilizing the MSTP on a network will have a single MSTP configuration that will have the following three attributes:

a) A configuration name defined by an alphanumeric string of up to 32 characters (defined in **the config stp mst_config_id** command as *name* <*string*>).

b) A configuration revision number (named here as a *revision_level*) and;

c) A 4096 element table (defined here as a *vid_range*) which will associate each of the possible 4096 VLANs supported by the Switch for a given instance.

To utilize the MSTP function on the Switch, three steps need to be taken:

a) The Switch must be set to the MSTP setting (*config stp version*)

b) The correct spanning tree priority for the MSTP instance must be entered (*config stp priority*).

c) VLANs that will be shared must be added to the MSTP Instance ID (*config stp instance_id*).

The Multiple Spanning Tree Protocol commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable stp	
disable stp	
config stp version	[mstp | rstp | stp]
config stp	{maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-2> | forwarddelay <value 4-30>| txholdcount <value 1-10> | fbpdu [enable | disable] |nni_bpdu_addr [dot1d | dot1ad]}(1)
config stp ports	<portlist> {externalCost [auto |<value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | p2p [true | false |auto] | restricted_tcn [true | false] | restricted_role [true | false] | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable |disable]}(1)
create stp instance_id	<value 1-15>
config stp instance_id	<value 1-15> [add_vlan | remove_vlan] <vidlist>
delete stp instance_id	<value 1-15>
config stp priority	<value 0-61440> instance_id <value 0-15>
config stp mst_config_id	{revision_level <int 0-65535> | name <string>}(1)
config stp mst_ports	<portlist> instance_id <value 0-15> {internalCost [auto | value 1-200000000] | priority <value 0-240>}(1)

Command	Parameters
show stp	
show stp ports	{<portlist>}
show stp instance	{<value 0-15>}
show stp mst_config_id	

Each command is listed, in detail, in the following sections.

enable stp

Purpose	Used to globally enable STP on the Switch.
Syntax	**enable stp**
Description	This command allows the Spanning Tree Protocol to be globally enabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable STP, globally, on the Switch:

```
DGS-3700-12:5#enable stp
Command: enable stp

Success.

DGS-3700-12:5#
```

disable stp

Purpose	Used to globally disable STP on the Switch.
Syntax	**disable stp**
Description	This command allows the Spanning Tree Protocol to be globally disabled on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable STP on the Switch:

```
DGS-3700-12:5#disable stp
Command: disable stp

Success.

DGS-3700-12:5#
```

config stp version

Purpose	Used to globally set the version of STP on the Switch.
Syntax	**config stp version [mstp | rstp | stp]**
Description	This command allows the user to choose the version of the spanning tree to be implemented on the Switch.
Parameters	*mstp* – Selecting this parameter will set the Multiple Spanning Tree Protocol (MSTP) globally on the Switch. *rstp* – Selecting this parameter will set the Rapid Spanning Tree Protocol (RSTP) globally on the Switch. *stp* – Selecting this parameter will set the Spanning Tree Protocol (STP) globally on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the Switch globally for the Multiple Spanning Tree Protocol (MSTP):

```
DGS-3700-12:5#config stp version mstp
Command: config stp version mstp

Success

DGS-3700-12:5#
```

config stp

Purpose	Used to setup STP, RSTP and MSTP on the Switch.
Syntax	**{maxage <value 6-40> | maxhops <value 1-20> | hellotime <value 1-2> | forwarddelay <value 4-30>| txholdcount <value 1-10> | fbpdu [enable | disable] |nni_bpdu_addr [dot1d | dot1ad]}(1)**
Description	This command is used to setup the Spanning Tree Protocol (STP) for the entire Switch. All commands here will be implemented for the STP version that is currently set on the Switch.
Parameters	*maxage <value 6-40>* – This value may be set to ensure that old information does not endlessly circulate through redundant paths in the network, preventing the effective propagation of the new information. Set by the Root Bridge, this value will aid in determining that the Switch has spanning tree configuration values consistent with other devices on the bridged LAN. If the value ages out and a BPDU has still not been received from the Root Bridge, the Switch will start sending its own BPDU to all other switches for permission to become the Root Bridge. If it turns out that your switch has the lowest Bridge Identifier, it will become the Root Bridge. The user may choose a time between *6* and *40* seconds. The default value is *20*. *maxhops <value 1-20>* – The number of hops between devices in a spanning tree region before the BPDU (bridge protocol data unit) packet sent by the Switch will be discarded. Each switch on the hop count will reduce the hop count by one until the value reaches zero. The Switch will then discard the BDPU packet and the information held for the port will age out. The user may set a hop count from *1* to *20*. The default is *20*. *hellotime <value 1-2>* – The user may set the time interval between transmission of configuration messages by the root device, thus stating that the Switch is still functioning. A time between *1* and *2* seconds may be chosen, with a default setting of *2* seconds. **NOTE:** In MSTP, the spanning tree is configured by port and therefore, the *hellotime* must be set using the *configure stp ports* command for switches utilizing the Multiple Spanning Tree Protocol. *forwarddelay <value 4-30>* – The maximum amount of time (in seconds) that the root device will wait before changing states. The user may choose a time between *4* and *30* seconds. The default is *15* seconds. *txholdcount <value 1-10>* – The maximum number of BPDU Hello packets transmitted per interval. Default value is *6*. *fbpdu [enable | disable]* – Allows the forwarding of STP BPDU packets from other network devices when STP is disabled on the Switch. The default is *enable*. *nni_bpdu_addr [dot1d | dot1ad]* – Configure NNI port address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure STP with maxage 18 and maxhops of 15:

```
DGS-3700-12:5#config stp maxage 18 maxhops 15
Command: config stp maxage 18 maxhops 15

Success.

DGS-3700-12:5#
```

config stp ports

Purpose	Used to setup STP on the port level.
Syntax	**config stp ports <portlist> {externalCost [auto | <value 1-200000000>] | hellotime <value 1-2> | migrate [yes | no] | edge [true | false | auto] | restricted_tcn [true | false] | restricted_role [true | false] | p2p [true | false | auto] | state [enable | disable] | fbpdu [enable |disable]}(1)**

config stp ports

Description	This command is used to create and configure STP for a group of ports.
Parameters	*<portlist>* – Specifies a range of ports to be configured. *externalCost* – This defines a metric that indicates the relative cost of forwarding packets to the specified port list. Port cost can be set automatically or as a metric value. The default value is *auto*. *auto* – Setting this parameter for the external cost will automatically set the speed for forwarding packets to the specified port(s) in the list for optimal efficiency. Default port cost: 100Mbps port = 200000. Gigabit port = 20000. <*value 1-200000000*> – Define a value between 1 and 200000000 to determine the external cost. The lower the number, the greater the probability the port will be chosen to forward packets. *hellotime <value 1-2>* – The time interval between transmission of configuration messages by the designated port, to other devices on the bridged LAN, thus stating that the Switch is still functioning. The user may choose a time between 1 and *2* seconds. The default is 2 seconds. *migrate [yes | no]* – Setting this parameter as "*yes*" will set the ports to send out BDPU packets to other bridges, requesting information on their STP setting If the Switch is configured for RSTP, the port will be capable to migrate from 802.1D STP-compatible to 802.1D RSTP. If the Switch is configured for MSTP, the port is capable of migrating from 802.1D STP-compatible to 802.1Q MSTP. RSTP and MSTP can coexist with standard STP, however the benefits of RSTP and MSTP are not realized on a port where an 802.1D network connects to an 802.1D-2004 or 802.1Q enabled network. Migration should be set as *yes* on ports connected to network stations or segments that are capable of being upgraded to 802.1D-2004 RSTP or 802.1Q MSTP on all or some portion of the segment. *edge [true | false | auto]* – *true* designates the port as an edge port. Edge ports cannot create loops, however an edge port can lose edge port status if a topology change creates a potential for a loop. An edge port normally should not receive BPDU packets. If a BPDU packet is received it automatically loses edge port status. *false* indicates that the port does not have edge port status. *Auto* – Will indicate that the port will be able to automatically enable edge port status if needed. *restricted_role [true | false]* – If *true* causes the Port not to be selected as Root Port for the CIST or any MSTI, even it has the best spanning tree priority vector. Such a Port will be selected as an Alternate Port after the Root Port has been selected. This parameter should be *false* by default. If set, it can cause lack of spanning tree connectivity. It is set by a network administrator to prevent bridges external to a core region of the network influencing the spanning tree active topology, possibly because those bridges are not under the full control of the administrator. *restricted_tcn [true | false]* – If *true* causes the Port not to propagate received topology change notifications and topology changes to other Ports. This parameter should be *false* by default. If set it can cause temporary loss of connectivity after changes in a spanning trees active topology as a result of persistent incorrectly learned station location information. It is set by a network administrator to prevent bridges external to a core region of the network, causing address flushing in that region, possibly because those bridges are not under the full control of the administrator or MAC_Operational for the attached LANs transitions frequently. *p2p [true | false | auto]* – *true* indicates a point-to-point (P2P) shared link. P2P ports are similar to edge ports however they are restricted in that a P2P port must operate in full-duplex. Like edge ports, P2P ports transition to a forwarding state rapidly thus benefiting from RSTP. A p2p value of false indicates that the port cannot have p2p status. *Auto* allows the port to have p2p status whenever possible and operate as if the p2p status were *true*. If the port cannot maintain this status (for example if the port is forced to half-duplex operation) the p2p status changes to operate as if the p2p value were *false*. The default setting for this parameter is *auto*. *state [enable | disable]* – Allows STP to be enabled or disabled for the ports specified in the port list. The default is *enable*. *fbpdu [enable | disable]* – When enabled, this allows the forwarding of STP BPDU packets from other network devices when STP is disabled in the specified ports. If users want to enable Forwarding BPDU on a per port basis, the following settings must first be in effect: 1.

config stp ports

	STP must be globally disabled and 2. Forwarding BPDU must be globally enabled. To globally disable STP, use the **disable stp** command, to globally enable fbpdu, use the **config stp** command. The default is *enable.*
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure STP with path cost 19, hellotime set to 2 seconds, migration enabled, and state enabled for ports 1-5:

```
DGS-3700-12:5#config stp ports 1-5 externalCost 19 hellotime 2 migrate yes state
enable
Command: config stp ports 1-5 externalCost 19 hellotime 2 migrate yes state enable

Success.

DGS-3700-12:5#
```

create stp instance_id

Purpose	Used to create a STP instance ID for MSTP.
Syntax	**create stp instance_id <value 1-15>**
Description	This command allows the user to create a STP instance ID for the Multiple Spanning Tree Protocol. There are 16 STP instances on the Switch (one internal CIST, unchangeable) and the user may create up to 15 instance IDs for the Switch.
Parameters	*<value 1-15>* – Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a spanning tree instance 2:

```
DGS-3700-12:5#create stp instance_id 2
Command: create stp instance_id 2

Warning:There is no VLAN mapping to this instance_id!
Success.

DGS-3700-12:5#
```

config stp instance_id

Purpose	Used to add or delete VID to/from an STP instance.
Syntax	**config stp instance_id <value 1-15> [add_vlan | remove_vlan] <vidlist>**
Description	This command is used to map VIDs (VLAN IDs) to previously configured STP instances on the Switch by creating an *instance_id*. A STP instance may have multiple members with the same MSTP configuration. There is no limit to the number of STP regions in a network but each region only supports a maximum of 16 spanning tree instances (one unchangeable default entry). VIDs can belong to only one spanning tree instance at a time.  **NOTE:** Switches in the same spanning tree region having the same STP *instance_id* must be mapped identically, and have the same configuration *revision_level* number and the same *name*.
Parameters	*<value 1-15>* – Enter a number between 1 and 15 to define the *instance_id*. The Switch supports 16 STP instances with one unchangeable default instance ID set as *0*. *add_vlan* – Along with the *vid_range <vidlist>* parameter, this command will add VIDs to the previously configured STP *instance_id.* *remove_vlan* – Along with the *vid_range <vidlist>* parameter, this command will remove VIDs to the previously configured STP *instance_id.* *<vidlist>* – Specify the VID range from configured VLANs set on the Switch. Supported VIDs on the Switch range from ID number 1 to 4094.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure instance ID 2 to add VID 10:

```
DGS-3700-12:5#config stp instance_id 2 add_vlan 10
Command : config stp instance_id 2 add_vlan 10

Success.

DGS-3700-12:5#
```

Example usage:

To remove VID 10 from instance ID 2:

```
DGS-3700-12:5#config stp instance_id 2 remove_vlan 10
Command : config stp instance_id 2 remove_vlan 10

Success.

DGS-3700-12:5#
```

delete stp instance_id

Purpose	Used to delete a STP instance ID from the Switch.
Syntax	**delete stp instance_id <value 1-15>**
Description	This command allows the user to delete a previously configured STP instance ID from the Switch.
Parameters	*<value 1-15>* – Enter a value between 1 and 15 to identify the Spanning Tree instance on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete STP instance ID 2 from the Switch.

```
DGS-3700-12:5#delete stp instance_id 2
Command: delete stp instance_id 2

Success.

DGS-3700-12:5#
```

config stp priority

Purpose	Used to configure the bridge priority.
Syntax	**config stp priority <value 0-61440> instance_id <value 0-15>**
Description	This command is used to update the STP instance configuration settings on the Switch. The MSTP will utilize the priority in selecting the root bridge, root port and designated port. Assigning higher priorities to STP regions will instruct the Switch to give precedence to the selected *instance_id* for forwarding packets. The lower the priority value set, the higher the priority.
Parameters	*priority <value 0-61440>* – Select a value between 0 and 61440 to specify the priority for a specified instance ID for forwarding packets. The lower the value, the higher the priority. This value must be divisible by 4096. *instance_id <value 0-15>* – Enter the value corresponding to the previously configured instance ID of which the user wishes to set the priority value. An instance id of *0* denotes the default *instance_id* (CIST) internally set on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the priority value for *instance_id* 2 as 4096.

```
DGS-3700-12:5#config stp priority 4096 instance_id 2
Command : config stp priority 4096 instance_id 2

Success.

DGS-3700-12:5#
```

config stp mst_config_id

Purpose	Used to update the MSTP configuration identification.
Syntax	**config stp mst_config_id {revision_level <int 0-65535> | name <string>}(1)**
Description	This command will uniquely identify the MSTP configuration currently configured on the Switch. Information entered here will be attached to BPDU packets as an identifier for the MSTP region to which it belongs. Switches having the same *revision_level* and *name* will be considered as part of the same MSTP region.
Parameters	*revision_level <int 0-65535>*– Enter a number between 0 and 65535 to identify the MSTP region. This value, along with the name will identify the MSTP region configured on the Switch. The default setting is *0*. *name <string>* – Enter an alphanumeric string of up to 32 characters to uniquely identify the MSTP region on the Switch. This *name*, along with the *revision_level* value will identify the MSTP region configured on the Switch. If no *name* is entered, the default name will be the MAC address of the device.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the MSTP region of the Switch with *revision_level* 10 and the *name* "Trinity":

```
DGS-3700-12:5#config stp mst_config_id revision_level 10 name Trinity
Command : config stp mst_config_id revision_level 10 name Trinity

Success.

DGS-3700-12:5#
```

config stp mst_ports

Purpose	Used to update the port configuration for a MSTP instance.
Syntax	**config stp mst_ports <portlist> instance_id <value 0-15> {internalCost [auto | <value 1-200000000>] priority <value 0-240>}(1)**
Description	This command will update the port configuration for a STP *instance_id*. If a loop occurs, the MSTP function will use the port priority to select an interface to put into the forwarding state. Set a higher priority value for interfaces to be selected for forwarding first. In instances where the priority value is identical, the MSTP function will implement the lowest MAC address into the forwarding state and other interfaces will be blocked. Remember that lower priority values mean higher priorities for forwarding packets.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *instance_id <value 0-15>* – Enter a numerical value between 0 and 15 to identify the *instance_id* previously configured on the Switch. An entry of 0 will denote the CIST (Common and Internal Spanning Tree. *internalCost* – This parameter is set to represent the relative cost of forwarding packets to specified ports when an interface is selected within a STP instance. The default setting is *auto*. There are two options: *auto* – Selecting this parameter for the internalCost will set quickest route automatically and optimally for an interface. The default value is derived from the media speed of the interface. *value 1-200000000* – Selecting this parameter with a value in the range of 1-200000000 will set the quickest route when a loop occurs. A lower *internalCost* represents a quicker transmission. *priority <value 0-240>* – Enter a value between 0 and 240 to set the priority for the port interface. A higher priority will designate the interface to forward packets first. A lower number denotes a higher priority. This value must be divisible by 16.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To designate ports 1 through 5, with instance id 2, to have an auto internalCost and a priority of 16:

```
DGS-3700-12:5#config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16
Command : config stp mst_ports 1-5 instance_id 2 internalCost auto priority 16

Success.

DGS-3700-12:5#
```

show stp

Purpose	Used to display the Switch's current STP configuration.
Syntax	**show stp**
Description	This command displays the Switch's current STP configuration.
Parameters	None.
Restrictions	None.

Example usage:

To display the status of STP on the Switch:

Status 1: STP enabled with STP compatible version

```
DGS-3700-12:5#show stp
Command: show stp

 STP Bridge Global Settings
 --------------------------
 STP Status          : Enabled
 STP Version         : STP compatible
 Max Age             : 18
 Hello Time          : 2
 Forward Delay       : 15
 Max Hops            : 15
 TX Hold Count       : 6
 Forwarding BPDU     : Disabled
 NNI BPDU Address    : dot1d

DGS-3700-12:5#
```

Status 2 : STP enabled for RSTP

```
DGS-3700-12:5#show stp
Command: show stp

 STP Bridge Global Settings
 --------------------------
 STP Status          : Enabled
 STP Version         : RSTP
 Max Age             : 20
 Hello Time          : 2
 Forward Delay       : 15
 Max Hops            : 20
 TX Hold Count       : 6
 Forwarding BPDU     : Disabled
 NNI BPDU Address    : dot1d

DGS-3700-12:5#
```

Status 3 : STP enabled for MSTP

```
DGS-3700-12:5#show stp
Command: show stp

 STP Bridge Global Settings
 --------------------------
 STP Status          : Enabled
 STP Version         : MSTP
 Max Age             : 18
 Forward Delay       : 15
 Max Hops            : 15
 TX Hold Count       : 6
 Forwarding BPDU     : Disabled
 NNI BPDU Address    : dot1d

DGS-3700-12:5#
```

show stp ports

Purpose	Used to display the Switch's current STP ports configuration.
Syntax	**show stp ports <portlist>**
Description	This command displays the STP ports settings for a specified port or group of ports (one port at a time).
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed. Information for a single port is displayed. If no ports are specified the STP information for port 1 will be displayed. Users may use the Space bar, p and n keys to view information for the remaining ports.
Restrictions	None.

Example usage:

To show STP ports information for port 1 (STP enabled on Switch):

```
DGS-3700-12:5#show stp ports
Command: show stp ports

MSTP Port Information
 ----------------------
 Port Index     : 1     , Hello Time: 2 /2 , Port STP : Enabled  ,
 External PathCost : 1             , Edge Port : False/No , P2P : Auto /Yes
 Port RestrictedRole : False,  Port RestrictedTCN : False
 Port Forward BPDU : Enabled
 MSTI  Designated Bridge  Internal PathCost Prio Status     Role
 ----- ----------------- ----------------- ---- --------- ----------
 0      N/A                 20000           128  Disabled  Disabled
 1      N/A                 200000          128  Disabled  Disabled
 2      N/A                 200000          128  Disabled  Disabled

DGS-3700-12:5#
```

show stp instance_id

Purpose	Used to display the Switch's STP instance configuration
Syntax	**show stp instance_id <value 0-15>**
Description	This command displays the Switch's current STP Instance Settings and the STP Instance Operational Status.
Parameters	*<value 0-15>* – Enter a value defining the previously configured *instance_id* on the Switch. An entry of *0* will display the STP configuration for the CIST internally set on the Switch.
Restrictions	None.

Example usage:

To display the STP instance configuration for instance 0 (the internal CIST) on the Switch:

```
DGS-3700-12:5#show stp instance 0
Command: show stp instance 0

STP Instance Settings
 --------------------------
 Instance Type          : CIST
 Instance Status        : Enabled
 Instance Priority      : 32768(Bridge Priority : 32768, SYS ID Ext : 0 )

 STP Instance Operational Status
 -------------------------------
 Designated Root Bridge : 4096 /00-11-95-AA-41-00
 External Root Cost     : 200004
 Regional Root Bridge   : 32768/00-01-02-03-04-00
 Internal Root Cost     : 0
 Designated Bridge      : 32768/00-50-BA-97-D9-56
 Root Port              : 7
 Max Age                : 20
 Forward Delay          : 15
 Last Topology Change   : 0
 Topology Changes Count : 21

DGS-3700-12:5#
```

show stp mst_config_id

Purpose	Used to display the MSTP configuration identification.
Syntax	**show stp mst_config_id**
Description	This command displays the Switch's current MSTP configuration identification.
Parameters	None.
Restrictions	None.

Example usage:

To show the MSTP configuration identification currently set on the Switch:

```
DGS-3700-12:5#show stp mst_config_id
Command: show stp mst_config_id

Current MST Configuration Identification
---------------------------------------------------------

Configuration Name : 00:53:13:1A:33:24     Revision Level :0
MSTI ID     Vid list
-------    -----------
CIST        2-4094
1           1

DGS-3700-12:5#
```

38

FORWARDING DATABASE COMMANDS

The layer 2 forwarding database commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
create fdb	<vlan_name 32> <macaddr> port <port>
create multicast_fdb	<vlan_name 32> <macaddr>
config multicast_fdb	<vlan_name 32> <macaddr> [add | delete] <portlist>
config fdb aging_time	<sec 10-1000000>
delete fdb	<vlan_name 32> <macaddr>
clear fdb	[vlan <vlan_name 32> | port <port> | all]
show multicast_fdb	{vlan <vlan_name 32> | mac_address <macaddr>}
show fdb	{port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}
config multicast vlan_filtering_mode	[vlanid <vidlist>|vlan <vlan_name 32>| all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]
show multicast vlan_filtering_mode	{[vlanid <vidlist>|vlan <vlan_name 32>]}

Each command is listed, in detail, in the following sections.

create fdb

Purpose	Used to create a static entry to the unicast MAC address forwarding table (database).
Syntax	**create fdb <vlan_name 32> <macaddr> port <port>**
Description	This command will make an entry into 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 that will be added to the forwarding table. *port <port>* – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a unicast MAC FDB entry**:**

```
DGS-3700-12:5#create fdb default 00-00-00-00-01-02 port 5
Command: create fdb default 00-00-00-00-01-02 port 5

Success.

DGS-3700-12:5#
```

create multicast_fdb

Purpose	Used to create a static entry to the multicast MAC address forwarding table (database)
Syntax	**create multicast_fdb <vlan_name 32> <macaddr>**
Description	This command will make an entry into the Switch's multicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the forwarding table.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create multicast MAC forwarding**:**

```
DGS-3700-12:5#create multicast_fdb default 01-00-00-00-00-01
Command: create multicast_fdb default 01-00-00-00-00-01

Success.

DGS-3700-12:5#
```

config multicast_fdb

Purpose	Used to configure the Switch's multicast MAC address forwarding database.
Syntax	**config multicast_fdb <vlan_name 32> <macaddr> [add | delete] <portlist>**
Description	This command configures the multicast MAC address forwarding table.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that will be added to the multicast forwarding table. *[add | delete]* – *add* will add ports to the forwarding table. *delete* will remove ports from the multicast forwarding table. *<portlist>* – Specifies a port or range of ports to be configured.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To add multicast MAC forwarding:

```
DGS-3700-12:5#config multicast_fdb default 01-00-00-00-00-01 add 1-5
Command: config multicast_fdb default 01-00-00-00-00-01 add 1-5

Success.

DGS-3700-12:5#
```

config fdb aging_time

Purpose	Used to set the aging time of the forwarding database.
Syntax	**config fdb aging_time <sec 10-1000000>**
Description	This command 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 10 to 1000000 seconds with a default value of 300 seconds. 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 10-1000000>* – The aging time for the MAC address forwarding database value. The value in seconds may be between 10 and 1000000 seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the FDB aging time:

```
DGS-3700-12:5#config fdb aging_time 300
Command: config fdb aging_time 300

Success.

DGS-3700-12:5#
```

delete fdb

Purpose	Used to delete an entry to the Switch's forwarding database.
Syntax	**delete fdb <vlan_name 32> <macaddr>**
Description	This command is used to delete a previous entry to 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 that will be added to the forwarding table.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a permanent FDB entry:

```
DGS-3700-12:5#delete fdb default 00-00-00-00-01-02
Command: delete fdb default 00-00-00-00-01-02

Success.

DGS-3700-12:5#
```

To delete a multicast FDB entry:

```
DGS-3700-12:5#delete fdb default 01-00-00-00-01-02
Command: delete fdb default 01-00-00-00-01-02

Success.

DGS-3700-12:5#
```

clear fdb

Purpose	Used to clear the Switch's forwarding database of all dynamically learned MAC addresses.
Syntax	**clear fdb [vlan <vlan_name 32> | port <port> | all]**
Description	This command is used to clear dynamically learned entries to the Switch's forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *port <port>* – The port number corresponding to the MAC destination address. The Switch will always forward traffic to the specified device through this port. *all* – Clears all dynamic entries to the Switch's forwarding database.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear all FDB dynamic entries**:**

```
DGS-3700-12:5#clear fdb all
Command: clear fdb all

Success.

DGS-3700-12:5#
```

show multicast_fdb

Purpose	Used to display the contents of the Switch's multicast forwarding database.
Syntax	**show multicast_fdb [vlan <vlan_name 32> | mac_address <macaddr>]**
Description	This command is used to display the current contents of the Switch's multicast MAC address forwarding database.
Parameters	*<vlan_name 32>* – The name of the VLAN on which the MAC address resides. *<macaddr>* – The MAC address that is present in the forwarding database table.
Restrictions	None.

Example usage:

To display multicast MAC address table:

```
DGS-3700-12:5#show multicast_fdb vlan default
Command: show multicast_fdb vlan default

 VLAN Name       : default
 MAC Address     : 01-00-00-00-00-01
 Egress Ports    : 1-5
 Mode            : Static

Total Entries: 1

DGS-3700-12:5#
```

show fdb

Purpose	Used to display the current unicast MAC address forwarding database.
Syntax	**show fdb {port <port> | vlan <vlan_name 32> | mac_address <macaddr> | static | aging_time}**
Description	This command will display the current contents of the Switch's forwarding database.
Parameters	*port* <*port*> – The port number corresponding to the MAC destination address. The Switch will always forward 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 that is present in the forwarding database table. *static* – Displays the static MAC address entries. *aging_time* – Displays the aging time for the MAC address forwarding database.
Restrictions	None.

Example usage:

To display unicast MAC address table:

```
DGS-3700-12:5#show fdb
Command: show fdb

  Unicast MAC Address Aging Time  = 300

   VID  VLAN Name          MAC Address       Port  Type
   ---- ---------------- ----------------- ----- -----------------
   1    default           00-00-00-1B-FC-02 7     Dynamic
   1    default           00-00-00-E0-06-09 7     Dynamic
   1    default           00-00-48-CD-25-3A 7     Dynamic
   1    default           00-00-5E-00-01-01 7     Dynamic
   1    default           00-00-5E-00-01-5F 7     Dynamic
   1    default           00-00-81-00-00-01 7     Dynamic
   1    default           00-00-81-9A-F2-F4 7     Dynamic
   1    default           00-00-C8-CD-25-3A 7     Dynamic
   1    default           00-00-E2-2F-44-EC 7     Dynamic
   1    default           00-00-EB-A4-50-5A 7     Dynamic
   1    default           00-00-F0-78-EB-00 7     Dynamic
   1    default           00-00-FC-0E-34-3E 7     Dynamic
   1    default           00-01-02-03-04-00 CPU   Self
   1    default           0-01-06-30-00-00 7      Dynamic
   1    default           00-01-10-FE-0D-14 7     Dynamic
```

config multicast vlan_filtering_mode

Purpose	Used to configure the the multicast packet filtering mode for VLANs.
Syntax	**config multicast vlan_filtering_mode [vlanid <vidlist>|vlan <vlan_name 32>| all] [forward_all_groups | forward_unregistered_groups | filter_unregistered_groups]**
Description	This command is used to configure the multicast packet filtering mode for VLANs. Port filtering mode and VLAN filtering mode are mutual exclusive.
Parameters	*vlanid_list* – Specifies a range of VLANs to be configured. *vlan_name* – Specifies the name of the VLANs to be configured. The filtering mode can be any of the following: *forward_all_groups* *forward_unregistered_groups* *filter_unregistered_groups*
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the multicast packet filtering mode for VLANs:

```
DGS-3700-12:5#config multicast vlan_filtering_mode vlanid 200-300 forward_all_groups
Command: config multicast vlan_filtering_mode vlanid 200-300 forward_all_groups

Success.

DGS-3700-12:5#
```

show multicast vlan_filtering_mode

Purpose	Used to show the multicast packet filtering mode for VLANs.
Syntax	**show multicast vlan_filtering_mode {[vlanid < vidlist > | vlan <vlan_name 32>]}**
Description	This command is used to display the multicast packet filtering mode for VLAN.
Parameters	*vlanid_list* – Specifies a range of vlans to be configured. If no parameter specified , the deivce will show all multicast filtering settings in the device.
Restrictions	None.

Example usage:

To display multicast VLAN filtering mode for VLANs:

```
DGS-3700-12:5#show multicast vlan_filtering_mode
Command: show multicast vlan_filtering_mode

VLAN ID/VLAN Name                          Multicast Filter Mode
-----------------------------------------  ----------------------------
1   /default                               forward_unregistered_groups
3   /RG                                    forward_unregistered_groups

DGS-3700-12:5#
```

39

LLDP COMMANDS

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

Command	Parameters
enable lldp	
disable lldp	
config lldp	message_tx_interval <sec 5 - 32768 >
config lldp	message_tx_hold_multiplier < 2 – 10 >
config lldp	tx_delay < sec 1 - 8192 >
config lldp	reinit_delay < sec 1 - 10 >
config lldp	notification_interval <sec 5 - 3600 >
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}(1)] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_pvid [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]
config lldp ports	[<portlist>|all] dot1_tlv_ protocol_identity[all | { eapol | lacp | gvrp | stp }(1)] [enable | disable]
config lldp ports	[<portlist>|all] dot3_tlvs [all | {mac_phy_configuration_status | link aggregation | maximum_frame_size}(1)] [enable | disable]
config lldp	forward_message [enable | disable]
show lldp	
show lldp mgt_addr	{[ipv4 <ipaddr> | ipv6 <ipv6addr>]}
show lldp ports	{<portlist>}
show lldp local_ports	{ <portlist>} {mode [brief | normal | detailed]}
show lldp remote_ports	{<portlist>} {mode [brief | normal | detailed]}
show lldp statistics	
show lldp statistics ports	{<portlist>}

Each command is listed, in detail, in the following sections.

enable lldp

Purpose	Used to enable LLDP operation on the Switch.
Syntax	**enable lldp**
Description	This is a global control for the LLDP function. When this function is enabled, the switch can start to transmit LLDP packets and receive and process the LLDP packets. The specific function of each port will depend on the per port LLDP settings. For the advertisement of LLDP packets, the switch announces the information to its neighbor through ports. For the receiving of LLDP packets, the switch will learn the information from the LLDP packets advertised from the neighbor in the neighbor table. The default state for LLDP is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable LLDP:

```
DGS-3700-12:5#enable lldp
Command: enable lldp

Success.

DGS-3700-12:5#
```

disable lldp

Purpose	Used to disable LLDP operation on the Switch.
Syntax	**disable lldp**
Description	This command will stop the sending and receiving of LLDP advertisement packets on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable LLDP:

```
DGS-3700-12:5#disable lldp
Command: disable lldp

Success.

DGS-3700-12:5#
```

config lldp message_tx_interval

Purpose	Used to change the packet transmission interval.
Syntax	**config lldp message_tx_interval <sec 5 – 32768>**
Description	This command controls how often active ports retransmit advertisements to their neighbors.
Parameters	*message_tx_interval* – Changes the interval between consecutive transmissions of LLDP advertisements on any given port. The range is from *5* seconds to *32768* seconds. The default setting is *30* seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To show the packet transmission interval:

```
DGS-3700-12:5#config lldp message_tx_interval 30
Command: config lldp message_tx_interval 30

Success.

DGS-3700-12:5#
```

config lldp message_tx_hold_multiplier

Purpose	Used to configure the message hold multiplier.
Syntax	**config lldp message_tx_hold_multiplier < 2 - 10 >**
Description	This command is a multiplier on the msgTxInterval that is used to compute the TTL value of txTTL in an LLDPDU. TheTTL will be carried in the LLDPDU packet. The lifetime will be the minimum of 65535 and (message_tx_interval * message_tx_hold_multiplier). At the partner switch, when the tme-to-Live for a given advertisement expires, the advertised data is deleted from the neighbor switch's MIB.
Parameters	*message_hold_multiplier* – The range is from *2* to *10*. The default setting is *4*.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To change the multiplier value:

```
DGS-3700-12:5#config lldp message_tx_hold_multiplier 3
Command: config lldp message_tx_ hold_multiplier 3

Success.

DGS-3700-12:5#
```

config lldp tx_delay

Purpose	Used to change the minimum time (delay-interval) any LLDP port will delay advertising successive LLDP advertisements due to a change in LLDP MIB content. The tx_delay defines the minimum interval between sending of LLDP messages due to constantly change of MIB content.
Syntax	**config lldp tx_delay < sec 1–8192 >**
Description	The LLDP message_tx_interval (transmit interval) must be greater than or equal to (4 x tx_delay interval).
Parameters	*tx_delay* – The range is from *1* second to *8192* seconds. The default setting is *2* seconds. NOTE: txDelay should be less than or equal to 0.25 * msgTxInterval.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the delay interval:

```
DGS-3700-12:5#config lldp tx_delay 8
Command: config lldp tx_delay 8

Success.

DGS-3700-12:5#
```

config lldp reinit_delay

Purpose	Change the minimum time of the reinitialization delay interval.
Syntax	**config lldp reinit_delay <sec 1 - 10>**
Description	An re-enabled LLDP port will wait for reinit_delay after last disable command before reinitializing.
Parameters	*reinit_delay* – The range is from *1* second to *10* seconds. The default setting is *2* seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To changes the re-initialization delay interval to five seconds:

```
DGS-3700-12:5#config lldp reinit_delay 5
Command: config lldp reinit_delay 5

Success.

DGS-3700-12:5#
```

config lldp notification _interval

Purpose	Used to configure the timer of the notification interval for sending notification to configured SNMP trap receiver(s).
Syntax	**config lldp notification_interval <sec 5 – 3600 >**
Description	This command is used to globally change the interval between successive LLDP change notifications generated by the switch.
Parameters	*notification_interval* – The range is from *5* seconds to *3600* seconds. The default setting is *5* seconds.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To change the notification interval to 10 seconds:

```
DGS-3700-12:5#config lldp notification_interval 10
Command: config lldp notification_interval 10

Success.

DGS-3700-12:5#
```

config lldp ports notification

Purpose	Used to configure each port for sending notification to configured SNMP trap receiver(s).
Syntax	**config lldp ports [<portlist>|all] notification [enable | disable]**
Description	This command is used to enable or disable each port for sending changes notification to configured SNMP trap receiver(s) if an LLDP data change is detected in an advertisement received on the port from an LLDP neighbor. The definition of change includes new available information, information timeout, information update. And the changed type includes any data update /insert/remove.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *notification* – Enables or disables the SNMP trap notification of LLDP data changes detected on advertisements received from neighbor devices. The default notification state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To change the SNMP notification state of ports 1 to 5 to enable:

```
DGS-3700-12:5#config lldp ports 1-5 notification enable
Command: config lldp ports 1-5 notification enable

Success.

DGS-3700-12:5#
```

config lldp ports admin_status

Purpose	Used to configure per-port transmit and receive modes.
Syntax	**config lldp ports [<portlist>|all] admin_status [tx_only | rx_only | tx_and_rx | disable]**
Description	This command is used to enable the user to control which ports participate in LLDP traffic and whether the participating ports allow LLDP traffic in only one direction or in both directions.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *admin_status* – *tx_only* – Configure the specified port(s) to transmit LLDP packets, but block inbound LLDP packets from neighbor devices. *rx_only* – Configure the specified port(s) to receive LLDP packets from neighbors, but block outbound packets to neighbors. *tx_and_rx* – Configure the specified port(s) to both transmit and receive LLDP packets. *disable* – Disable LLDP packet transmit and receive on the specified port(s). The default per port state is *tx_and_rx*.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure ports 1 to 5 to transmit and receive:

```
DGS-3700-12:5#config lldp ports 1-5 admin_status rx_and_tx
Command: config lldp ports 1-5 admin_status rx_and_tx

Success.

DGS-3700-12:5#
```

config lldp ports mgt_addr

Purpose	Used to enable or disable port(s) specified for advertising indicated management address instance.
Syntax	**config lldp ports [<portlist>|all] mgt_addr [ipv4 <ipaddr> | ipv6 <ipv6addr>] | [enable | disable]**
Description	This command specifies whether the system's IP address needs to be advertised from the specified port. For layer 3 devices, each managed address can be individually specified. The management addresses that are added in the list will be advertised in the LLDP from the specified interface associated with each management address. The interface for that management address will be also advertised in the if-index Form
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *ipv4* – The IP address of IPv4. *ipv6* – The IP address of IPv6. *[enable|disable]* – enable or disable the specified ports that manage the address entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To enable ports 1 to 2 to manage address entry:

```
DGS-3700-12:5#config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable
Command: config config lldp ports 1-2 mgt_addr ipv4 192.168.254.10 enable

Success.

DGS-3700-12:5#
```

config lldp ports basic_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more optional TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] basic_tlvs [all | {port_description | system_name | system_description | system_capabilities}] [enable | disable]**
Description	An active LLDP port on the switch always includes the mandatory data in its outbound advertisements. And there are four optional data that can be configured for an individual port or group of ports to exclude one or more of these data types from outbound LLDP advertisements. The mandatory data type include four basic types of information (end of LLDPDU TLV, chassis ID TLV, port ID TLV, and Time to Live TLV). The mandatory type can not be disabled. There are also four data types which can be optionally selected. They are *port_description*, *system_name*, *system_description*, and *system_capability*.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *port_description* – This TLV optional data type indicates that LLDP agent should transmit 'Port Description TLV on the port. The default state is disabled. *system_name* – This TLV optional data type indicates that LLDP agent should transmit 'System Name TLV'. The default state is disabled. *system_description* – This TLV optional data type indicates that LLDP agent should transmit 'System Description TLV'. The default state is disabled. *system_capabilities* – This TLV optional data type indicates that LLDP agent should transmit 'System Capabilities TLV'. The system capability will indicate whether the device provides repeater, bridge, or router function, and whether the provided functions are currently enabled. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure exclude the system name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3700-12:5#config lldp ports all basic_tlvs system_name enable
Command: config lldp ports all basic_tlvs system_name enable

Success.

DGS-3700-12:5#
```

config lldp dot1_tlv_pvid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_pvid [enable | disable]**
Description	This command is used to determine whether the IEEE 802.1 organizationally defined port VLAN TLV transmission is allowed on a given LLDP transmission capable port.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_pvid* – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the VLAN nameTLV from the outbound LLDP advertisements for all ports:

```
DGS-3700-12:5#config lldp ports all dot1_tlv_pvid enable
Command: config lldp ports all dot1_tlv_pvid enable

Success.

DGS-3700-12:5#
```

config lldp dot1_tlv_protocol_vid

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally port and protocol VLAN ID TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_protocol_vid [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]**
Description	This command is used to indicate whether the corresponding Local System's port and protocol VLAN ID instance will be transmitted on the port. If a port is associated with multiple protocol VLANs, those enabled port and protocol VLAN IDs will be advertised.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_protocol_vid* – This TLV optional data type determines whether the IEEE 802.1 organizationally defined port and protocol VLAN ID TLV transmission is allowed on a given LLDP transmission capable port. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the port and protocol VLAN ID TLV from the outbound LLDP advertisements for all ports:

```
DGS-3700-12:5#config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_protocol_vid vlanid 1-3 enable

Success.

DGS-3700-12:5#
```

config lldp dot1_tlv_vlan_name

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally VLAN name TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_vlan_name [vlan [all | <vlan_name 32>] | vlanid <vlanid_list>] [enable | disable]**
Description	This command is used to indicate whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN IDs will be advertised.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_vlan_name* – This TLV optional data type indicates whether the corresponding Local System's VLAN name instance will be transmitted on the port. If a port is associated with multiple VLANs, those enabled VLAN IDs will be advertised. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure exclude the VLAN name TLV from the outbound LLDP advertisements for all ports:

```
DGS-3700-12:5#config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable
Command: config lldp ports all dot1_tlv_vlan_name vlanid 1-3 enable

Success.

DGS-3700-12:5#
```

config lldp dot1_tlv_protocol_identity

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.1 Organizationally protocol identity TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot1_tlv_ protocol_identity [all | {eapol | lacp | gvrp | stp }(1)] [enable | disable]**
Description	This command is used to indicate whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol identity will be advertised.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *dot1_tlv_protocol_identity* – This TLV optional data type indicates whether the corresponding Local System's Protocol Identity instance will be transmitted on the port. The Protocol Identity TLV provides a way for stations to advertise protocols that are important to the operation of the network. Such as Spanning Tree Protocol, the Link Aggregation Control Protocol, and numerous vendor proprietary variations are responsible for maintaining the topology and connectivity of the network. If EAPOL, GVRP, STP(including MSTP), and LACP protocol identity is enabled on this port and it is enabled to be advertised, then this protocol

config lldp dot1_tlv_protocol_identity

	identity will be advertised. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the protocol identity TLV from the outbound LLDP advertisements for all ports:

```
DGS-3700-12:5#config lldp ports all dot1_tlv_protocol_identity all enable
Command: config lldp ports all dot1_tlv_protocol_identity all enable

Success.

DGS-3700-12:5#
```

config lldp dot3_tlvs

Purpose	Used to configure an individual port or group of ports to exclude one or more of IEEE 802.3 Organizationally Specific TLV data types from outbound LLDP advertisements.
Syntax	**config lldp ports [<portlist>|all] dot3_tlvs [all | {mac_phy_configuration_status | link_aggregation | maximum_frame_size}] [enable | disable]**
Description	This command is used to enable each Specific TLV in this extension individually.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *all* – Use this parameter to set all ports in the system. *mac_phy_configuration_status* – This TLV optional data type indicates that LLDP agent should transmit 'MAC/PHY configuration/status TLV'. This type indicates it is possible for two ends of an IEEE 802.3 link to be configured with different and/or speed settings and still establish some limited network connectivity. More precisely, the information includes whether the port support the auto-negotiation function, whether the function is enabled, the auto-negotiated advertised capability, and the operational MAU type. The default state is disabled. *link_aggregation* – This TLV optional data type indicates that LLDP agent should transmit 'Link Aggregation TLV'. This type indicates the current link aggregation status of IEEE 802.3 MACs. More precisely, the information should include whether the port is capable of doing link aggregation, whether the port is aggregated in a aggregated link, and the aggregated port ID. The default state is disabled. *power_via_mdi* – This TLV optional data type indicates that the LLDP agent should transmit 'Power via MDI TLV'. Three IEEE 802.3 PMD implementations (10BASE-T, 100BASE-TX, and 1000BASE-T) allow power to be supplied over the link for connected non-powered systems. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending IEEE 802.3 LAN station. The default state is disabled. Note: Not supported in the current release. *maximum_frame_size* – This TLV optional data type indicates that LLDP agent should transmit 'Maximum-frame-size TLV. The default state is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure exclude the MAC/PHY configuration/status TLV from the outbound LLDP advertisements for all ports:

```
DGS-3700-12:5#config lldp ports all dot3_tlvs mac_phy_configuration_status enable
Command: config lldp ports all dot3_tlvs mac_phy_configuration_status enable

Success.

DGS-3700-12:5#
```

config lldp forward_message

Purpose	Used to configure the forwarding of LLDPDU packets when LLDP is disabled.
Syntax	**config lldp forward_message [enable | disable]**
Description	When LLDP is disabled and LLDP forward_message is enabled, the received LLDPDU packets will be forwarded. The default state is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage Example:

To configure LLDP forward_message:

```
DGS-3700-12:5#config lldp forward_message enable
Command: config lldp forward_message enable

Success.

DGS-3700-12:5#
```

show lldp

Purpose	This command displays the switch's general LLDP configuration status.
Syntax	**show lldp**
Description	This command displays the switch's general LLDP configuration status.
Parameters	None.
Restrictions	None.

Usage Example:

To display the LLDP system level configuration status:

```
DGS-3700-12:5#show lldp
Command: show lldp

LLDP System Information
    Chassis ID Subtype        : MAC Address
    Chassis ID                : 00-01-02-03-04-00
    System Name               :
    System Description        : Gigabit Ethernet Switch
    System Capabilities       : Repeater, Bridge

LLDP Configurations
    LLDP Status               : Disabled
    LLDP Forward Status       : Disabled
    Message Tx Interval       : 30
    Message Tx Hold Multiplier : 4
    ReInit Delay              : 2
    Tx Delay                  : 2
    Notification Interval     : 5

DGS-3700-12:5#
```

show lldp mgt_addr

Purpose	Used to display the LLDP management address information.
Syntax	**show lldp mgt_addr {[ipv4 <ipaddr> | ipv6 <ipv6addr>]}**
Description	This command is used to display the LLDP management address information.
Parameters	*ipv4* – The IP address of IPv4. *ipv6* – The IP address of IPv6.
Restrictions	None.

Example usage:

To display management address information for port 1:

```
DGS-3700-12:5#show lldp mgt_addr ipv4 192.168.254.10
Command: show lldp mgt_addr ipv4 192.168.254.10

Address 1
-------------------------------------------------
      Subtype      : IPv4
      Address      : 192.168.254.10
      IF type      : Unknown
      OID          : 1.3.6.1.4.1.171.10.36.1.11
      Advertising Ports : 1-5,7

DGS-3700-12:5#
```

show lldp ports

Purpose	Display the LLDP per port configuration for advertisement options.
Syntax	**show lldp ports {<portlist>}**
Description	This command displays the LLDP per port configuration for advertisement options.
Parameters	*<portlist>* – Use this parameter to define ports to be configured.
Restrictions	None.

Example usage:

To display the LLDP per port TLV option configuration:

```
DGS-3700-12:5#show lldp ports 1
Command: show lldp ports 1

Port ID                 : 1
------------------------------------------------------------------
Admin Status            : TX_and_RX
Notification Status     : Disabled
Advertised TLVs Option  :
    Port Description                                    Disabled
    System Name                                         Disabled
    System Description                                  Disabled
    System Capabilities                                 Disabled
    Enabled Management Address
        (None)
    Port VLAN ID                                        Disabled
    Enabled Port_and_Protocol_VLAN_ID
        (None)
    Enabled VLAN Name
        (None)
    Enabled Protocol_Identity
        (None)
    MAC/PHY Configuration/Status                        Disabled
    Link Aggregation                                    Disabled
    Maximum Frame Size                                  Disabled

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

show lldp local_ports

Purpose	Used to display the per-port information currently available for populating outbound LLDP advertisements.
Syntax	**show lldp local_ports {<portlist>} {mode [brief | normal | detailed]}**
Description	This command displays the per-port information currently available for populating outbound LLDP advertisements.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *brief* – Display the information in brief mode. *normal* – Display the information in normal mode. This is the default display mode. *detailed* – Display the information in detailed mode.
Restrictions	None.

Usage Example:

To display outbound LLDP advertisements for port 1-2:

```
DGS-3700-12:5#show lldp local_ports 1-2
Command: show lldp local_ports 1-2

Port ID : 1
------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : 1/1
Port Description                         : RMON Port  1 on Unit 1
Port PVID                                : 1
Management Address Count                 : 1
PPVID Entries Count                      : 0
VLAN Name Entries Count                  : 1
Protocol Identity Entries Count          : 0
MAC/PHY Configuration/Status             : (See Detail)
Link Aggregation                         : (See Detail)
Maximum Frame Size                       : 1536

Port ID : 2
------------------------------------------------------------------
Port ID Subtype                          : Local
Port ID                                  : 1/2
Port Description                         : RMON Port  2 on Unit 1
Port PVID                                : 1
Management Address Count                 : 1
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

show lldp remote_ports

Purpose	Used to display the information learned from the neighbor.
Syntax	**show lldp remote_ports {<portlist>} {mode [brief | normal | detailed]}**
Description	This command is used to display the information learned from the neighbor parameters. Due to a memory limitation, only 32 VLAN Name entries and 10 Management Address entries can be received.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. *mode* – Choose from three options: *brief* – Display the information in brief mode. *normal* – Display the information in normal mode. This is the default display mode. *detailed* – Display the information in detailed mode.
Restrictions	None.

Example usage:

To display remote table in brief mode:

```
DGS-3700-12:5#show lldp remote_ports 1-2 mode brief
Command: show lldp remote_ports 1-2 mode brief

Port ID: 1
---------------------------------------------------
Remote Entities Count   : 1
Entity 1
     Chassis ID Subtype     : MAC Address
     Chassis ID             : 00-01-0-2-03-04-01
     Port ID Subtype        : Local
     Port ID                : 1/3
     Port Description       : RMON Port 1 on Unit 3

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

show lldp statistics

Purpose	Used to display the system LLDP statistics information.
Syntax	**show lldp statistics**
Description	This command is used to display an overview of neighbor detection activity on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To display global statistics information:

```
DGS-3700-12:5#show lldp statistics
Command: show lldp statistics

Last Change Time       : 1110
Number of Table Insert : 0
Number of Table Delete : 0
Number of Table Drop   : 0
Number of Table Ageout : 0

DGS-3700-12:5#
```

show lldp statistics ports

Purpose	Used to display the ports LLDP statistics information.
Syntax	**show lldp statistics ports{<portlist>}**
Description	This command is used to display per-port LLDP statistics.
Parameters	*<portlist>* – Use this parameter to define ports to be configured. When portlist is not specified, information for all ports will be displayed.
Restrictions	None.

Usage Example:

To display statistics information of port 1:

```
DGS-3700-12:5#show lldp statistics ports 1
Command: show lldp statistics ports 1

Port ID : 1
-----------------------------------------------
    LLDPStatsTxPortFramesTotal           : 0
    LLDPStatsRxPortFramesDiscardedTotal  : 0
    LLDPStatsRxPortFramesErrors          : 0
    LLDPStatsRxPortFramesTotal           : 0
    LLDPStatsRxPortTLVsDiscardedTotal    : 0
    LLDPStatsRxPortTLVsUnrecognizedTotal : 0
    LLDPStatsRxPortAgeoutsTotal          : 0

DGS-3700-12:5#
```

40

CONNECTIVITY FAULT MANAGEMENT COMMANDS

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

Command	Parameters
create cfm md	<string 22> level <int 0-7>
config cfm md	<string 22> {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}(1)
create cfm ma	<string 22> md <string 22>
config cfm ma	<string 22> md <string 22> {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}(1)
create cfm mep	<string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward | outward] port <port>
config cfm mep	[mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centiseconds 250 -1000> | alarm_reset_time <centiseconds 250-1000>}(1)
delete cfm mep	[mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>]
delete cfm ma	<string 22> md <string 22>
delete cfm md	<string 22>
enable cfm	
disable cfm	
config cfm ports	<portlist> state [enable | disable]
show cfm ports	<portlist>
show cfm	{[md <string 22> {ma <string 22> {mepid <int 1-8191>}} | mepname <string 32>]}
show cfm remote_mep	[mepname <string 32> | md <string 22> ma <string 22> mepid <int 1-8191>] remote_mepid <int 1-8191>
show cfm fault	{md <string 22> {ma <string 22>}}
show cfm port	<port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}
show cfm mipccm	
show cfm pkt_cnt	{[ports <portlist>{rx | tx}] | rx | tx | ccm}
clear cfm pkt_cnt	{[ports <portlist>{rx | tx}] | rx | tx | ccm}
cfm loopback	<macaddr> [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}
cfm linktrace	<macaddr> [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {ttl <int 2-255> | pdu_priority <int 0-7>}
show cfm linktrace	[mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {trans_id <uint>}
delete cfm linktrace	{[md <string 22> {ma <string 22> {mepid <int 1-8191>}} | mepname <string 32>]}
config cfm ccm_fwd	[software | hardware]

Command	Parameters
show cfm ccm_fwd	
config cfm mp_ltr_all	[enable | disable]
show cfm mp_ltr_all	

Each command is listed, in detail, in the following sections.

create cfm md

Purpose	Used to create a maintenance domain.
Syntax	**create cfm md <string 22> level <int 0-7>**
Description	Different maintenance domains should have different names.
Parameters	*md* – Specifies the maintenance domain name. *level* – Specifies the maintenance domain level.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a CFM maintenance domain.

```
DGS-3700-12:5#create cfm md op_domain level 2
Command: create cfm md op_domain level 2

Success.

DGS-3700-12:5#
```

config cfm md

Purpose	Used to configure parameters of a maintenance domain.
Syntax	**config cfm md <string 22> {mip [none | auto | explicit] | sender_id [none | chassis | manage | chassis_manage]}(1)**
Description	Creation of MIPs on a MA is useful for tracing the link MIP by MIP. It also allows the user to perform loop-back from MEP to an MIP.
Parameters	*md* – Specifies the maintenance domain name. *mip* – Specifies and controls the creation of MIPs. *none* – Specifies that MIPs will not be created. This is the default value. *auto* – MIPs can always be created on any ports in this MD, if that port is not configured with a MEP of this MD. For the intermediate switch in a MA, the setting must be auto in order for the MIPs to be created on this device. *explicit* – MIPs can be created on any ports in this MD, only if the existing lower level has an MEP configured on that port, and that port is not configured with an MEP of this MD.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure CFM on a maintenance domain:

```
DGS-3700-12:5#config cfm md op_domain mip explicit
Command: config cfm md op_domain mip explicit

Success.

DGS-3700-12:5#
```

create cfm ma

Purpose	Used to create a maintenance association.
Syntax	**create cfm ma <string 22> md <string 22>**
Description	Different MAs in a MD must have different MA Names. Different MAs in different MDs may have the same MA Name.
Parameters	*md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a CFM maintenance association:

```
DGS-3700-12:5#create cfm ma op1 md op_domain
Command: create cfm ma op1 md op_domain

Success.

DGS-3700-12:5#
```

config cfm ma

Purpose	Used to configure a maintenance association.
Syntax	**config cfm ma <string 22> md <string 22> {vlanid <vlanid 1-4094> | mip [none | auto | explicit | defer] | sender_id [none | chassis | manage | chassis_manage | defer] | ccm_interval [10ms | 100ms | 1sec | 10sec | 1min | 10min] | mepid_list [add | delete] <mepid_list>}(1)**
Description	The MEP list specified for a MA can be located in different devices. MEPs must be created on ports of these devices explicitly. An MEP will transmit CCM packets periodically across the MA. The receiving MEP will verify these received CCM packets from other MEPs against this MEP list for the configuration integrity check.
Parameters	*md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name. *vlanid* – Specifies the VLAN Identifier. Different MAs must be associated with different VLANs. *mip* – Specifies the control creation of MIPs. *none* – No MIPs will be created. *auto* – MIPs can always be created on any ports in this MA, if that port is not configured with an MEP of that MA. *explicit* – MIP can be created on any ports in this MA, only if the next existent lower level has a MEP configured on that port, and that port is not configured with a MEP of this MA. *defer* – Inherit the settings configured for the maintenance domain that this MA is associated with. This is the default value. *ccm_interval* – Specifies the CCM interval. *10ms* – 10 milliseconds. Not recommended. For test purposes. *100ms* – 100 milliseconds. Not recommended. For test purposes. *1sec* – One second. *10sec* – Ten seconds. This is the default value. *1min* – One minute. *10min* – Ten minutes. *mepid* – Specify the MEPIDs contained in the maintenance association. The range of MEPID is 1-8191. *add* – Add MEPID(s). *delete* – Specifies to delete MEPID(s). By default, there's no MEPID in a newly created maintenance association.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure CFM maintenance association:

```
DGS-3700-12:5#config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec
Command: config cfm ma op1 md op_domain vlanid 1 ccm_interval 1sec

Success.

DGS-3700-12:5#
```

create cfm mep

Purpose	Used to create a cfm MEP.
Syntax	**create cfm mep <string 32> mepid <int 1-8191> md <string 22> ma <string 22> direction [inward | outward] port <port>**
Description	Different MEP in the same MA must have different MEP ID. MD name, MA name, and MEP ID together can identify a MEP. Different MEP on the same device must have a different MEP name. Before an MEP is created, its MEPID should be configured in MA's MEPID list.
Parameters	*mep* – Specifies the MEP name. It's unique among all MEPs configured on the device. *mepid* – Specifies the MEP MEPID. It should be configured in MA's MEPID list. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name. *direction* – Specifies the MEP direction. *inward* – Specifies the inward facing (up) MEP. *outware* – Specifies the outward facing (down) MEP. *port* – Specifies the port number. This port should be a member of the MA's associated VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a CFM MEP.

```
DGS-3700-12:5#create cfm mep mep1 mepid 1 md op_domain ma op1 direction
inward port 2
Command: create cfm mep mep1 mepid 1 md op_domain ma op1 direction inward port 2

Success.

DGS-3700-12:5#
```

config cfm mep

Purpose	Used to configure parameters of a MEP.
Syntax	**config cfm mep [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {state [enable | disable] | ccm [enable | disable] | pdu_priority <int 0-7> | fault_alarm [all | mac_status | remote_ccm | error_ccm | xcon_ccm | none] | alarm_time <centiseconds 250 -1000> | alarm_reset_time <centiseconds 250-1000>}(1)**
Description	An MEP may generate 5 types of Fault Alarms, as shown below by their priorities from high to low: Cross-connect CCM Received: priority 5 Error CCM Received: priority 4 Some Remote MEP Down: priority 3 Some Remote MEP MAC Status Error: priority 2 Some Remote MEP Defect Indication: priority 1 If multiple types of faults occurr on a MEP, only the fault of the highest priority will be alarmed.
Parameters	*mepname* – Specifies the MEP name. It's unique among all MEPs configured on the device. *mepid* – Specifies the MEP MEPID. It should be configured in MA's MEPID list. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name. *state* – Specifies the MEP administrative state. *enable* – MEP is enabled. *disable* – MEP is disabled. This is the default value. *ccm* – Specifies the CCM transmission state. *enable* – CCM transmission enabled. *disable* – CCM transmission disabled. This is the default value. *pdu_priority* – Specifies the 802.1p priority to be set in CCMs and LTMs messages transmitted by the MEP. The default value is 7. *fault_alarm* – Control types of fault alarms sent by the MEP. *all* – Specifies that all types of fault alarms will be sent. *mac_status* – Only Fault Alarms whose priority is equal to or higher than "Some Remote MEP MAC Status Error" will be sent. *remote_ccm* – Only Fault Alarms whose priority is equal to or higher than "Some Remote MEP Down" will be sent. *error_ccm* – Only Fault Alarms whose priority is equal to or higher than "Error CCM Received" will be sent. *xcon_ccm* – Only Fault Alarms whose priority is equal to or higher than "Cross-connect CCM Received" will be sent. *none* – No fault alarm is sent. This is the default value. *alarm_time* – The time that a defect must last before the fault alarm can be sent. The default value is 2 seconds. *alarm_reset_time* – The timer must be clear of any alarm defects before the fault can be re-alarmed. The default value is 10 seconds
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the CFM mep:

```
GS-3700-12:5#config cfm mep mepid 1 md 1 ma 1 state enable ccm enable
Command: config cfm mep mepid 1 md 1 ma 1 state enable ccm enable

Success.

DGS-3700-12:5#
```

delete cfm mep

Purpose	Used to delete a created MEP.
Syntax	**delete cfm mep [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>]**
Description	This command is used to delete a created MEP.
Parameters	*mepname* – Specifies the MEP name. It's unique among all MEPs configured on the device. *mepid* – Specifies the MEP MEPID. It should be configured in MA's MEPID list. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete CFM mep:

```
DGS-3700-12:5#delete cfm mep mepname mep1
Command: delete cfm mep mepname mep1

Success.

DGS-3700-12:5#
```

delete cfm ma

Purpose	Used to delete a created maintenance association.
Syntax	**delete cfm ma <string 22> md <string 22>**
Description	All MEPs created in the maintenance association will be deleted automatically.
Parameters	*md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a CFM ma:

```
DGS-3700-12:5#delete cfm ma op1 md 3
Command: delete cfm ma op1 md 3

Success.

DGS-3700-12:5#
```

delete cfm md

Purpose	Used to delete a created maintenance domain.
Syntax	**delete cfm md <string 22>**
Description	All MEPs and maintenance associations created in the maintenance domain will be deleted automatically.
Parameters	md – Specifies the maintenance domain name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a CFM md:

```
DGS-3700-12:5#delete cfm md 3
Command: delete cfm md 3

Success.

DGS-3700-12:4#
```

enable cfm

Purpose	This command is used to enable CFM globally.
Syntax	**enable cfm**
Description	This command is used to enable CFM globally.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable CFM:

```
DGS-3700-12:5#enable cfm
Command: enable cfm

Success.

DGS-3700-12:5#
```

disable cfm

Purpose	Used to disable CFM globally.
Syntax	**disable cfm**
Description	This command is used to disable CFM globally.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable CFM:

```
DGS-3700-12:4# disable cfm
Command: disable cfm

Success.

DGS-3700-12:4#
```

config cfm ports

Purpose	Used to enable or disable CFM function on per-port basis.
Syntax	**config cfm ports <portlist> state [enable | disable]**
Description	By default, CFM function is disabled on all ports. If CFM is disabled on a port: • MIPs are never created on that port. • MEPs can still be created on that port, and the configuration can be saved. • MEPs created on that port can never generate or process CFM PDUs. If the user issues a Loop-back or Linktrace test on those MEPs, it will prompt user that CFM function is disabled on that port.
Parameters	*ports* – Specifies the logical port list. *state* – Is used to enable or disable CFM function.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure CFM ports:

```
DGS-3700-12:5#config cfm ports 2-5 state enable
Command: config cfm ports 2-5 state enable

Success.

DGS-3700-12:5#
```

show cfm ports

Purpose	This command is used to show cfm state of specified ports.
Syntax	**show cfm ports <portlist>**
Description	This command is used to display CFM state of speicified ports.
Parameters	*ports* – Specifies the logical port list.
Restrictions	None.

Example usage:

To display CFM ports:

```
DGS-3700-12:5#show cfm ports 3-6
Command: show cfm ports 3-6

Port   State
-----  --------
3      Enabled
4      Enabled
5      Enabled
6      Disabled

DGS-3700-12:5#
```

show cfm

Purpose	This command is used to show CFM information.
Syntax	**show cfm {[md <string 22> {ma <string 22> {mepid <int 1-8191>}} | mepname <string 32>]}**
Description	This command is used to show CFM information.
Parameters	*md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance domain name. *mepid* – Specifies the MEP MEPID. *mepname* – Specifies the MEP name.
Restrictions	None.

Example usage:

To display CFM:

```
DGS-3700-12:5#show cfm
Command: show cfm

CFM State: Enabled

Level  MD Name
-----  ----------------------
2      op_domain

DGS-3700-12:5#
```

Example usage:

To display CFM md:

```
DGS-3700-12:5#show cfm md op_domain
Command: show cfm md op_domain

MD Level    : 2
MIP Creation: Explicit
SenderID TLV: None
VID   MA Name
----  ----------
1     op1

DGS-3700-12:5#
```

Example usage:

To display CFM mepname:

```
DGS-3700-12:5#show cfm mepname mep1
Command: show cfm mepname mep1

Name                    : mep1
MEPID                   : 1
Port                    : 1
Direction               : inward
CFM Port State          : enabled
MAC Address             : XX-XX-XX-XX-XX-XX
MEP State               : enabled
CCM State               : enabled
PDU Priority            : 7
Fault Alarm             : mac_status
Alarm Time              : 2 second(s)
Alarm Reset Time        : 10 second(s)
Highest Fault           : Remote CCM
Next LTM Trans ID       : 27
RX Out-of-Sequence CCMs: 0
RX Cross-connect CCMs   : 0
RX Error CCMs           : 0
RX Port Status CCMs     : 0
RX If Status CCMs       : 0
RX In-order LBRs        : 0
TX CCMs                 : 1234
TX LBMs                 : 0

Remote MEP Status
MEPID  MAC Address Status RDI PortSt IfSt    Detect Time
------ ----------- ------ --- ------- -------- -------------------
2      XX-..-XX-XX OK     Yes Blocked Up      2008-01-01 12:00:00
3      XX-..-XX-XX IDLE   No  No      No      2008-01-01 12:00:00
4      XX-..-XX-XX OK     No  Up      Down    2008-01-01 12:00:00
8      XX-..-XX-XX START  No  Up      Up      2008-01-01 12:00:00
12     XX-..-XX-XX FAILED No  Up      Up      2008-01-01 12:00:00
8      XX-..-XX-XX OK     No  Up      Up      2008-01-01 12:00:00
DGS-3700-12:5#
```

show cfm fault

Purpose	This command is used to show fault MEPs.
Syntax	**show cfm fault {md <string 22> {ma <string 22>}}**
Description	This command is used to display all the fault conditions detected by the MEPs contained in the specified MA or MD. This display provides the overview of fault status by MEPs.
Parameters	*md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance domain name.
Restrictions	None.

Example usage:

To display CFM fault:

```
DGS-3700-12:4#show cfm mep fault
Command: show cfm mep fault

MD Name     MA Name     MEPID    Status
----------- ----------- ----- --------------------------
op_domain   op1         1        Cross-connect CCM Received

DGS-3700-12:4#
```

show cfm port

Purpose	This command is used to show MEPs and MIPs created on a port.
Syntax	**show cfm port <port> {level <int 0-7> | direction [inward | outward] | vlanid <vlanid 1-4094>}**
Description	This command is used to show MEPs and MIPs created on a port.
Parameters	*port* – Specifies the port number. *level* – Specifies the MD Level. If not specified, all levels are shown. *direction* – Specifies the MEP direction. *inward* – Inward facing MEP. *outward* – Outward facing MEP. If not specified, both directions and MIPs are shown. *Vlanid* – VLAN identifier. If not specified, all VLANs are shown.
Restrictions	None.

Example usage:

To display CFM ports:

```
DGS-3700-12:4#show cfm port 1
Command: show cfm port 1

MAC Address: 10:10:90:08:8g:12

MD Name     MA Name     MEPID Level Direction VID
----------- ----------- ----- ----- --------- ----
op_domain   op1         1     2     inward    2
cust_domain cust1       8     4     inward    2
serv_domain serv2       MIP   3               2


DGS-3700-12:4#
```

show cfm mipccm

Purpose	This command is used to show MIPCCM database entries.
Syntax	**show cfm mipccm**
Description	This command is used to display all entries in the MIPCCM. The MIPCCM entry is simlar to FDB which keeps the forwarding port information for a MAC entry.
Parameters	None.
Restrictions	None.

Example usage:

To display the MIPCCM database entries:

```
DGS-3700-12:5#show cfm mipccm
Command: show cfm mipccm

MA          VID   MAC Address        Port
----------  ----  -----------------  -----
opma        1     00-01-02-03-04-05  2
opma        1     00-01-02-03-04-05  3

Total: 2

DGS-3700-12:5#
```

cfm linktrace

Purpose	This command is used to issue a CFM linktrack message.
Syntax	**cfm linktrace <macaddr> [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {ttl <int 2-255> | pdu_priority <int 0-7>}**
Description	This command is used to issue a CFM linktrack message.
Parameters	*<macaddr>* – Specifies the destination MAC address. *mepname* – Specifies the MEP name. *mepid* – Specifies the MEP MEPID. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name. *ttl* – Specifies the linktrace message TTL value. The default value is 64. *pdu_priority* – The 802.1p priority to be set in the transmitted LTM. If not specified, it uses the same priority as CCMs sent by the MA.
Restrictions	None.

Example usage:

To create a CFM linktrace:

```
DGS-3700-12:4#cfm linktrace 00-01-02-03-04-05 mep mep1
Command: cfm linktrace 00-01-02-03-04-05 mep mep1

Transaction ID: 26
Success.

DGS-3700-12:4#
```

show cfm linktrace

Purpose	Used to show linktrace responses.
Syntax	**show cfm linktrace [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {trans_id <uint>}**
Description	The maximum linktrace responses a device can hold is 64.
Parameters	*<macaddr>* – Specifies the destination MAC address. *mepname* – Specifies the MEP name. *mepid* – MEP MEPID. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name. *trans_id* – Specifies the identifier of the transaction to show.
Restrictions	None.

Example usage:

To display the CFM linktrace:

```
DGS-3700-12:5#show cfm linktrace mep mep1
Command: show cfm linktrace mep mep1


Trans ID  Source MEP      Destination
--------- --------------- ------------------
26         mep1           00-01-02-03-04-05

DGS-3700-12:5#show cfm linktrace mep mep1 trans_id 26
Command: show cfm linktrace mep mep1 trans_id 26

Transaction ID: 26
From MEP mep1 to 00-01-02-03-04-05
Start Time 2008-01-01 12:00:00


Hop MEPID MAC Address      Forwarded  Relay Action
--- ---- ---------------- ---------  ------------
  -      00-01-02-03-04-05  Yes        FDB
  -      00-01-02-03-04-05  Yes        MPDB
8100     00-01-02-03-04-05  No         Hit


DGS-3700-12:5#
```

delete cfm linktrace

Purpose	This command is used to delete received linktrace responses.
Syntax	**delete cfm linktrace {[md <string 22> {ma <string 22> {mepid <int 1-8191>}} | mepname <string 32>]}**
Description	This command deletes the stored link trace response data that is initiated by the specified MEP.
Parameters	*mepname* – Specifies the MEP name. *mepid* – Specifies the MEP MEPID. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name.
Restrictions	None.

Example usage:

To delete a CFM linktrace:

```
DGS-3700-12:5#delete cfm linktrace mep mep1
Command: delete cfm linktrace mep mep1

Success.

DGS-3700-12:5#
```

config cfm ccm_fwd

Purpose	This command is used to configure CCM PDUs forwarding mode.
Syntax	**config cfm ccm_fwd [software | hardware]**
Description	This coommand is for test purposes. For ordinary user, it is not suggested to use this command. By default, the CCM message is handled and forwarded by software. The software can handle the packet based on behaviour defined by the standard. Under a strict environment, there may be substantial amount of CCM packets, and it will consume substantial amount of CPU resource. To meet the performance requirement, the handling of CCM can be changed to hardware mode. This function is especially useful for domain's intermediate device since they only have MIPS. Note that this command can only be used under assistance of technical personnel.
Parameters	*software* – Specifies to forward by software. *hardware* – Specifies to forward by hardware.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the CFM ccm forwarding mode:

```
DGS-3700-12:5#config cfm ccm_fwd_mode hardware
Command: config cfm ccm_fwd_mode hardware

Success.

DGS-3700-12:5#
```

cfm loopback

Purpose	Used to show MEPs and MIPs created on a port.
Syntax	**cfm loopback <macaddr> [mepname <string 32> | mepid <int 1-8191> md <string 22> ma <string 22>] {num <int 1-65535> | [length <int 0-1500> | pattern <string 1500>] | pdu_priority <int 0-7>}**
Description	The MAC address represents that the destination MEP or MIP which can be reached by this MAC address. The MEP represents the source MEP to initiate the loop-back message. You can press Ctrl+C to exit loop-back test.
Parameters	*<macaddr>* –Specifies the destination MAC address. *mepname* – Specifies the MEP name. *mepid* – Specifies the MEP MEPID. *md* – Specifies the maintenance domain name. *ma* – Specifies the maintenance association name. *num* – Specifies the number of LBMs to be sent. The default value is 4. *length* – Specifies the payload length of LBM to be sent. The default is 0. *pattern* – Specifies an arbitrary amount of data to be included in a Data TLV, along with an indication of whether the Data TLV is to be included. *pdu_priority* – The 802.1p priority to be set in the transmitted LBMs. If not specified, it uses the same priority as CCMs and LTMs sent by the MA.
Restrictions	None.

Example usage:

To configure CFM loop-back:

```
DGS-3700-12:4#cfm loopback 00-01-02-03-04-05 mep mep1
Command: cfm loopback 00-01-02-03-04-05 mep mep1

Request timed out.
Request timed out.
Reply from MPID 52: bytes=xxx time=xxxms
Request timed out.

CFM loopback statistics for 00-01-02-03-04-05:
    Packets: Sent=4, Received=1, Lost=3(75% loss).

DGS-3700-12:4#
```

show cfm pkt_cnt

Purpose	Used to show CFM packet RX/TX counters.
Syntax	**show cfm pkt_cnt {[ports <portlist>{rx | tx}] | rx | tx | ccm}**
Description	This command is used to display CFM packet counters.
Parameters	*ports* – Specifies which ports' counter to show. If not specified, all ports will be shown. *{rx | tx}* – Shows RX or TX packet counter. If none is specified, both of them are shown. *ccm* - Shows the CCM transmission state.
Restrictions	None.

Example usage:

The following example displays the statistics for CFM packets.

VidDrop: The packets dropped due to invalid VID.

OpcoDrop: The packets dropped due to unrecognized CFM opcode.

```
DGS-3700-12:5#show cfm counter packet
Command: show cfm counter packet

CFM RX Statistics
---------------------
Port  CCM      LBR      LBM      LTR      LTM      VidDrop OpcoDrop  Sum
----- -------- -------- -------- -------- -------- -------- -------- -----
1     0        0        0        0        0        0        0        0
2     254      0        0        0        0        0        0        254
3     0        0        0        0        0        0        0        0
4     0        0        0        0        0        0        0        0
5     0        0        0        0        0        0        0        0
6     0        0        0        0        0        0        0        0
7     0        0        0        0        0        0        0        0
8     0        0        0        0        0        0        0        0
9     0        3        0        0        0        0        0        3
10    0        0        0        0        0        0        0        0
11    0        0        0        0        0        0        0        0
12    0        0        0        0        0        0        0        0
Total 254      3        0        0        0        0        0        257


CFM TX Statistics
---------------------
Port    CCM      LBR      LBM      LTR      LTM      Sum
-----  -------- -------- -------- -------- --------  ------
1       0        0        0        0        0        0
2       284      0        0        0        4        292
3       578      0        0        0        0        578
4       578      0        0        0        0        578
5       578      0        0        0        0        578
6       578      0        0        0        0        578
```

clear cfm pkt_cnt

Purpose	Used to clear the CFM packet RX/TX counters.
Syntax	**clear cfm pkt_cnt {[ports <portlist>{rx | tx}] | rx | tx | ccm}**
Description	This command clears CFM packet counters.
Parameters	*ports* – Specifies which ports' counter to show. If not specified, all ports will be shown. *{rx | tx}* – Shows RX or TX packet counter. If none is specified, both of them are shown. *ccm* - Shows the CCM transmission state.
Restrictions	None.

Example usage:

To clear the CFM packet RX/TX counters:

```
DGS-3700-12:5#clear cfm pkt_cnt ports 2 rx
Command: clear cfm pkt_cnt ports 2 rx

Success.

DGS-3700-12:4#
```

config cfm mp_ltr_all

Purpose	To configure the CFM mp linktrace on the switch.
Syntax	**config cfm mp_ltr_all [enable | disable]**
Description	This command is used to configure the CFM mp linktrace on the switch.
Parameters	*enable* – Used to enable the CFM mp linktrace. *disable* – Used to disable the CFM mp linktrace.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure CFM mp linktrace:

```
DGS-3700-12:5#config cfm mp_ltr_all enable
Command: config cfm mp_ltr_all enable

Success.

DGS-3700-12:4#
```

show cfm mp_ltr_all

Purpose	To display the CFM mp linktrace settings on the switch.
Syntax	**show cfm mp_ltr_all**
Description	This command is used to display the CFM mp linktrace settings on the switch.
Parameters	None.
Restrictions	None.

Example usage:

To show the CFM mp linktrace on the Switch:

```
DGS-3700-12:4#show cfm mp_ltr_all
Command: show cfm mp_ltr_all

All MPs reply LTRs: Enabled

DGS-3700-12:4#
```

41

VLAN COUNTER COMMANDS

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

Command	Parameters
create vlan_counter	[vlan <vlan_name> | vlanid < vidlist >] {port [<port_list>|all] } [all_frame | broadcast | multicast | unicast] [packet | byte]
delete vlan_counter	[all | [vlan <vlan_name> | vlanid < vidlist >] [all | port <port_list> [all | [all_frame | broadcast | multicast | unicast][packet | byte]]]]
clear vlan_counter statistics	[all | [vlan <vlan_name> | vlanid < vidlist >] [all | port <port_list>]]
show vlan_counter	{[vlan <vlan_name> | vlanid < vidlist >]}
show vlan_counter statistics	{[vlan <vlan_name> | vlanid < vidlist >] {port <portlist>}}

Each command is listed, in detail, in the following sections.

create vlan_counter

Purpose	This command creates the control entry for VLAN traffic flow statistics.
Syntax	**create vlan_counter [vlan <vlan_name> | vlanid < vidlist >] {port [<port_list>|all] } [all_frame | broadcast | multicast | unicast] [packet | byte]**
Description	This command is used to create control entries to count statistics for specific VLANs, or to count statistics for specific ports on specific VLANs. The statistics can be either byte count or packet count. The statistics can be counted for different frame types.
Parameters	*vlan_name* – Specifies the VLAN name. *vidlist* – Specifies a list of VLANs by VLAN ID. *ports <port_list>* – To enable to count statistics by specific port on specific VLAN. *all_frame* – The statistics will be counted for all packets. *broadcast* – Specifies to count broadcast packets *multicast* – Specifies to count multicast packets *unicast* – Specifiesyo count unicast packets *packet* – Specifies to count at packet level. *byte* – Specifies to count at byte level.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To begin counting packet levels for broadcast packets on VLAN 1:

```
DGS-3700-12:5#create vlan_counter vlanid 1 broadcast packet
Command: create vlan_counter vlanid 1 broadcast packet

Success.

DGS-3700-12:5#
```

delete vlan_counter

Purpose	This command deletes the control entry for VLAN traffic flow statistics.
Syntax	**delete vlan_counter [all | [vlan <vlan_name> | vlanid < vidlist >] [all | port <port_list> [all | [all_frame | broadcast | multicast | unicast][packet | byte]]]]**
Description	This command deletes the control entry for VLAN traffic flow statistics.
Parameters	*all* – Specifies to delete all VLAN statistic control entries. *vlan_name* – Specifies the VLAN name. *vidlist* – Specifies a list of VLANs by VLAN ID. *ports <port_list>* – To disable to count statistics by specific port on specific VLAN. *all_frame* – The statistics will be stop counting for all packets. *broadcast* – Specifies to stop counting broadcast packets *multicast* – Specifies to stop counting multicast packets *unicast* – Specifies to stop counting unicast packets *packet* – Specifies to stop counting at packet level. *byte* – Specifies to stop counting at byte level.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To stop counting packet levels for broadcast packets on VLAN 1:

```
DGS-3700-12:5#delete vlan_counter vlanid 1 all
Command: delete vlan_counter vlanid 1 all

Success.

DGS-3700-12:5#
```

clear vlan_counter statistics

Purpose	Used to clear statistics gathered by the VLAN counter.
Syntax	**clear vlan_counter statistics [all | [vlan <vlan_name> | vlanid < vidlist >] [all | port <port_list>]]**
Description	This command is used to clear statistic gathered by the VLAN counter.
Parameters	*all* – Specifies to clear all VLAN statistics *vlan_name* – Specifies the VLAN name. *vidlist* – Specifies a list of VLANs by VLAN ID. *ports <port_list>* – To clear to count statistics by specific port on specific VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear statistics for VLAN 1-10:

```
DGS-3700-12:5#clear vlan_counter statistics vlanid 1-10 port 1-3
Command: clear vlan_counter statistics vlanid 1-10 port 1-3

Success.

DGS-3700-12:5#
```

show vlan_counter

Purpose	This commands displays the statistic control entries created for VLANs.
Syntax	**show vlan_counter {[vlan <vlan_name> | vlanid < vidlist >]}**
Description	This commands displays the statistic control entries created for VLANs.
Parameters	*vlan_name* – Specifies the VLAN name. *vlanid* – Specifies a list of VLANs by VLAN ID. When VLAN is not specified, all VLAN counters will be displayed.
Restrictions	None.

Example usage:

To display the statistic control entries:

```
DGS-3700-12:5#show vlan_counter vlanid 1-2
Command: show vlan_counter vlanid 1-2

VLAN ID  Ports           Packet Type  Counter Type
-------  --------------  -----------  ------------
1                        Broadcast    Packet

DGS-3700-12:5#
```

show vlan_counter statistics

Purpose	Displays the VLAN level receives packets or receive byte statistics.
Syntax	**show vlan_counter statistics {[vlan <vlan_name> | vlanid < vidlist >] {port <portlist>}}**
Description	This command displays the VLAN level receives packet or receive byte statistics.
Parameters	*vlan_name* – Specifies the VLAN name. *vlanid* – Specifies a list of VLANs by VLAN ID. When VLAN is not specified, all VLAN counters will be displayed.
Restrictions	None.

Example usage:

To display the VLAN counter statistic entries:

```
DGS-3700-12:5#show vlan_counter statistics vlanid 1-2
Command: show vlan_counter statistics vlanid 1-2

VLAN Port  Frame Type        RX Frames/RX Bytes  Frames Per Sec/Bytes Per Sec
==== ====  ================  ==================  ============================
1          Broadcast(Packet)  12335               23

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

42

ETHERNET OAM COMMANDS

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

Command	Parameters
config ethernet_oam ports mode	[<portlist> | all] mode [active | passive]
config ethernet_oam ports state	[<portlist> | all] state [enable | disable]
config ethernet_oam ports link_monitor error_symbol	[<portlist> | all] link_monitor error_symbol { threshold <number> | window < milliseconds 1000-60000> | notify_state [enable | disable]}(1)
config ethernet_oam ports link_monitor error_frame	[<portlist> | all] link_monitor error_frame { threshold <number> | window < milliseconds 1000-60000> | notify_state [enable | disable]}(1)
configure ethernet oam ports link_monitor error_frame_seconds	[<portlist> | all] link_monitor error_frame_seconds { threshold <number> | window < milliseconds 10000-900000> | notify_state [enable | disable]}(1)
config ethernet_oam ports link_monitor error_frame_period	[<portlist> | all] link_monitor error_frame_period { threshold <number> | window <number 148810-100000000> | notify_state [enable | disable]}(1)
config ethernet_oam ports critical_link_event	[<portlist> | all] critical_link_event [dying_gasp | critical_event] notify_state [enable | disable]
config ethernet_oam ports remote_loopback	[<portlist> | all] remote_loopback [start | stop]
config ethernet_oam ports received_remote_loopback	[<portlist> | all] received_remote_loopback [process | ignore]
show ethernet_oam ports status	{<portlist>}
show ethernet_oam ports configuration	{<portlist>}
show ethernet_oam ports statistics	{<portlist>}
clear ethernet_oam ports statistics	[<portlist>| all]
show ethernet oam event_log	{<portlist>} event_log {index <value_list> }
clear ethernet_oam ports event_log	[<portlist>| all]

Each command is listed, in detail, in the following sections.

config ethernet_oam ports mode

Purpose	Used to configure Ethernet OAM mode.
Syntax	**config ethernet_oam ports [<portlist> | all] mode [active | passive]**
Description	This command is used to configure ports Ethernet OAM to operate in active or passive mode. The following two actions are allowed by ports in active mode, but disallowed by ports in passive mode. Initiate OAM discovery and Start or stop remote loop-back. Note: When a port is OAM-enabled, changing the OAM mode will cause the OAM discovery to be re-started.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *mode* – Specifies to operate in either active mode or passive mode. The default mode is active.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 1 to OAM mode to passive:

```
DGS-3700-12:5#config ethernet_oam ports 1 mode passive
Command: config ethernet_oam ports 1 mode passive

Success.

DGS-3700-12:5#
```

config ethernet_oam ports state

Purpose	Used to enable or disable Ethernet OAM.
Syntax	**config ethernet_oam ports [<portlist> | all] state [enable | disable]**
Description	This command used to enable or disable the port's Ethernet OAM function. Enabling a port's OAM will cause the port to start OAM discovery. If a port is active, it initiates the discovery otherwise it reacts only to the discovery received from its peer. Disabling a port's OAM will cause the port to send out a dying gasp event to the peer and then disconnect the established OAM link.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *state* – Specifies to enable or disable the OAM function. The default state is disable.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable Ethernet OAM on port 1:

```
DGS-3700-12:5#config ethernet_oam ports 1 state enable
Command: config ethernet_oam ports 1 state enable

Success.

DGS-3700-12:5#
```

config ethernet_oam ports link_monitor error_symbol

Purpose	Used to configure Ethernet OAM link monitoring error symbols.
Syntax	**config ethernet_oam ports [<portlist> | all] link_monitor error_symbol{ threshold <number> | window < milliseconds 1000-60000> | notify_state [enable | disable](1)**
Description	This command is used to configure ports Ethernet OAM link monitoring error symbols. The link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the statistics on the number of frame errors as well as the number of coding symbol errors. When the number of symbol errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error symbol period event to notify the remote OAM peer.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *threshold* – Specifies the number of symbol errors in the period that is required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 symbol error. *window* – The range is 1000 to 60000 ms. The default value is 1000ms. *notify_state* – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and 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-3700-12:5#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-3700-12:5#
```

config ethernet_oam ports link_monitor error_frame

Purpose	Used to configure Ethernet OAM link monitoring error frame
Syntax	**config ethernet_oam ports [<portlist> | all] link_monitor error_frame { threshold < number > | window < milliseconds 1000-60000> | notify_state [enable | disable]}(1)**
Description	The command used to configure ports Ethernet OAM link monitoring error frames. Link monitoring function provides a mechanism to detect and indicate link faults under a variety of conditions. OAM monitors the counter on the number of frame errors as well as the number of coding symbol errors. When the number of frame errors is equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame event to notify the remote OAM peer.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *threshold* – Specifies the number of frame errors in the period that are required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 frame error. *window* – The range is 1000 to 60000 ms. The default value is 1000ms. *notify_state* – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the error frame threshold to 2 and period to 1000 ms for port 1:

```
DGS-3700-12:5#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-3700-12:5#
```

Configure Ethernet OAM link_monitor error_frame_seconds

Purpose	Used to configure Ethernet OAM link monitoring error frame seconds.
Syntax	**config ethernet_oam ports [<portlist> | all] link_monitor error_frame_seconds { threshold < number > | window < milliseconds 10000-900000> | notify_state [enable | disable]}(1)**
Description	This command is used to configure ports Ethernet OAM link monitoring error frame seconds. An error frame second is a 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 counter on the number of frame errors as well as the number of coding symbol errors. When the number of error frame seconds are equal to or greater than the specified threshold in a period and the event notification state is enabled, it generates an error frame second summary event to notify the remote OAM.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *threshold* – Specifies the number of error frame seconds in the period that are required to be equal to or greater than in order for the event to be generated. The default value of threshold is 1 error frame second. *window* – Specifies the period of error frame seconds summary event. The range is 10000ms-900000ms and the default value is 60000 ms. *notify_state* – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and 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-3700-12:5#config ethernet_oam ports 1 link_monitor error_frame_seconds threshold
2 window 10000 notify_state enable
Command: config ethernet_oam ports 1 link_monitor error_frame_seconds
threshold 2 window 10000 notify_state enable

Success.

DGS-3700-12:5#
```

config ethernet_oam ports link_monitor error_frame_period

Purpose	Used to configure the Ethernet OAM link monitoring error frame period.
Syntax	**config ethernet_oam ports [<portlist> | all] link_monitor error_frame_period { threshold < number > | window <number 148810-100000000> | notify_state [enable | disable]}(1)**
Description	This command is used to configure ports Ethernet OAM link monitoring error frame period. 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 error frames are 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.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify *all ports.* *threshold* – Specifies the number of error frame seconds in the period that are required to be equal to or greater than in order for the event to be generated. The default value of the threshold is 1 error frame. *window* – Specifies the period of the error frame period event. The period is specified by a number of received frames. The range for this setting is 148 810 to 100 000 000. The default value is 1 488 100 frames. *notify_state* – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the errored frame threshold to 10 and period to 1000000 for port 1:

```
DGS-3700-12:5#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-3700-12:5#
```

config ethernet_oam ports critical_link_event

Purpose	Used to configure Ethernet OAM critical link event.
Syntax	**config ethernet_oam ports [<portlist> | all] critical_link_event [dying_gasp | critical_event] notify_state [enable | disable]**
Description	This command is used to configure the capability of Ethernet OAM critical link event. If the capability for an event is disabled, the port will never send out the corresponding critical link event.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *dying_gasp* – An unrecoverable local failure condition has occurred. *critical_event* – An unspecified critical event has occurred. *Notify_state* – Specifies to enable or disable the event notification. The default state is enable.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure dying_gasp event for port 1:

```
DGS-3700-12:5#config ethernet_oam ports 1 critical_link_event dying_gasp
 notify_state enable
Command: config ethernet_oam ports 1 critical_link_event dying_gasp
notify_state enable

Success.

DGS-3700-12:5#
```

config ethernet_oam ports remote_loopback

Purpose	Used to start or stop Ethernet OAM remote loop-back .
Syntax	**config ethernet_oam ports [<portlist> | all] remote_loopback [start | stop]**
Description	This command is used to start or stop the remote peer to enter the Ethernet OAM remote loop-back mode. To start the remote peer to enter the remote loop-back mode, you must ensure the port is in active mode and the OAM connection is established. If the local client is already in remote loop-back mode, then it cannot apply this command.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *remote_loopback* – If start is specified, it will request the peer to change to the remote loop-back mode. If stop is specified, it will request the peer to change to the normal operation mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To start remote loop-back on port 1:

```
DGS-3700-12:5#config ethernet_oam ports 1 remote_loopback stop
Command: config ethernet_oam ports 1 remote_loopback stop

Success.

DGS-3700-12:5#
```

config ethernet_oam ports received_remote_loopback

Purpose	Used to configure the method to process the received Ethernet OAM remote loop-back command.
Syntax	**config ethernet_oam ports [<portlist> | all] received_remote_loopback [process | ignore]**
Description	This command is used to configure the client to process or to ignore the received Ethernet OAM remote loop-back command. In remote loop-back mode, all user traffic will not be processed. Ignoring received remote loop-back command will prevent the port from entering remote loop-back mode.
Parameters	*portlist* – Specifies a range of ports to be configured. Use *all* to specify all ports. *received_remote_loopback* – Specifies whether to process or to ignore the received Ethernet OAM remote loop-back command The default method is"ignore".
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the method of processing the received remote loop-back command as "process" on port 1:

```
DGS-3700-12:5#config ethernet_oam ports 1 received_remote_loopback process
Command: config ethernet_oam ports 1 received_remote_loopback process

Success.

DGS-3700-12:5#
```

show ethernet_oam ports status

Purpose	Used to show primary controls and status information for Ethernet OAM.
Syntax	**show ethernet_oam ports {<portlist>} status**
Description	This 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. See below values: **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 ports. 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. OAM mode change. (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 loop-back 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 At present, only loop-back and link monitoring are supported.
Parameters	*portlist* – Specifies a range of ports to display.
Restrictions	None

Example usage:

To show OAM control and status information on port 1-2:

```
DGS-3700-12:5#show ethernet_oam ports 1-2 status
DGS-3700-12:5#show ethernet_oam ports 1-2 status

Port 1
Local Client
-------------------------------------------------------------
  OAM                           : Enabled
  Mode                          : Passive
  Max OAMPDU                    : 1518  Bytes
  Remote Loopback               : Support
  Unidirection                  : Not Supported
  Link Monitoring               : Support
  Variable Request              : Not Supported
  PDU Revision                  : 1
  Operation Status              : LinkFault
  Loopback Status               : No Loopback

Port 2
Local Client
-------------------------------------------------------------
  OAM                           : Disabled
  Mode                          : Active
  Max OAMPDU                    : 1518  Bytes
  Remote Loopback               : Support
  Unidirection                  : Not Supported

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

show ethernet_oam ports configuration

Purpose	Used to display Ethernet OAM configuration.
Syntax	**show ethernet_oam ports {<portlist>} configuration**
Description	The command is used to show port's Ethernet OAM configurations.
Parameters	*portlist* – Specifies a range of ports to display.
Restrictions	None.

Example usage:

To show Ethernet OAM configuration on port 1-2:

```
DGS-3700-12:5#show ethernet_oam ports 1-2 configuration
Command: show ethernet_oam ports 1-2 configuration

Port 1
------------------------------------------------------------
OAM                     : Enabled
Mode                    : Passive
Dying Gasp              : Enabled
Critical Event          : Enabled
Remote Loopback OAMPDU  : Processed

Symbol Error
  Notify State            : Enabled
  Window:                 : 1000 milliseconds
  Threshold               : 2 Errored Symbol

Frame Error
  Notify State            : Enabled
  Window:                 : 1000 milliseconds
  Threshold               : 2 Errored Frame

Frame Period Error
  Notify State            : Enabled
  Window:                 : 1000000 Frames
  Threshold               : 10 Errored Frame

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

show ethernet_oam ports statistics

Purpose	This command is used to show Ethernet OAM statistics.
Syntax	**show ethernet_oam ports {<portlist>} statistics**
Description	This command is used to show ports Ethernet OAM statistics information.
Parameters	*portlist* – Specifies a range of ports to display.
Restrictions	None.

Example usage:

To show port 1 OAM statistics:

```
DGS-3700-12:5#show ethernet_oam ports 1 statistics
Command: show ethernet_oam ports 1 statistics

Port 1
------------------------------------------------------------
  Information OAMPDU Tx                 : 0
  Information OAMPDU Rx                 : 0
  Unique Event Notification OAMPDU Tx   : 0
  Unique Event Notification OAMPDU Rx   : 0
  Duplicate Event Notification OAMPDU Tx: 0
  Duplicate Event Notification OAMPDU Rx: 0
  Loopback Control OAMPDU Tx            : 0
  Loopback Control OAMPDU Rx            : 0
  Variable Request OAMPDU Tx            : 0
  Variable Request OAMPDU Rx            : 0
  Variable Response OAMPDU Tx           : 0
  Variable Response OAMPDU Rx           : 0
  Organization Specific OAMPDUs Tx      : 0
  Organization Specific OAMPDUs Rx      : 0
  Unsupported OAMPDU Tx                 : 0
  Unsupported OAMPDU Rx                 : 0
  Frames Lost Due To OAM                : 0

DGS-3700-12:5#
```

Show Ethernet OAM event_log

Purpose	Used to show the Ethernet OAM event log.
Syntax	**show ethernet_oam {<portlist>} event_log {index <value_list> }**
Description	This command is used to show 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. You can specify an index to show a range of events.
Parameters	*portlist* – Specifies a range of ports to display. *index* – Specifies an index range to display.
Restrictions	None.

Example usage:

To show port 1 external OAM event:

```
DGS-3700-12:5#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
   Dying Gasp                          : 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
   Dying Gasp                          : 0
   Critical Event                      : 0

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

clear ethernet_oam ports statistics

Purpose	Used to clear Ethernet OAM statistics.
Syntax	**clear ethernet_oam ports [<portlist>| all] statistics**
Description	This command is used to clear ports Ethernet OAM statistics information.
Parameters	*portlist* – Specifies a range of ports to clear the statistics.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear port 1 OAM statistics:

```
DGS-3700-12:5#clear ethernet_oam ports 1 statistics
Command: clear ethernet_oam ports 1 statistics

Success.

DGS-3700-12:5#
```

clear ethernet_oam ports event_log

Purpose	Used to clear Ethernet OAM event log
Syntax	**clear ethernet_oam ports [<portlist>| all] event_log**
Description	This command is used to clear ports Ethernet OAM event log information.
Parameters	*portlist* – Specifies a range of ports to clear the event log.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear port 1 OAM event:

```
DGS-3700-12:5#clear ethernet_oam ports 1 event_log
Command: clear ethernet_oam ports 1 event_log

Success.

DGS-3700-12:5#
```

43

QoS COMMANDS

The Switch supports 802.1p priority queuing. The Switch has 8 priority queues. These priority queues are numbered from 7 (Class 7) — the highest priority queue — to 0 (Class 0) — the lowest priority queue. The eight priority tags specified in IEEE 802.1p (p0 to p7) are mapped to the Switch's priority queues as follows:

- Priority 0 is assigned to the Switch's Q2 queue.
- Priority 1 is assigned to the Switch's Q0 queue.
- Priority 2 is assigned to the Switch's Q1 queue.
- Priority 3 is assigned to the Switch's Q3 queue.
- Priority 4 is assigned to the Switch's Q4 queue.
- Priority 5 is assigned to the Switch's Q5 queue.
- Priority 6 is assigned to the Switch's Q6 queue.
- Priority 7 is assigned to the Switch's Q7 queue.

Priority scheduling is implemented by the priority queues stated above. The Switch will empty the eight hardware priority queues in order, beginning with the highest priority queue, 7, to the lowest priority queue, 0. Each hardware queue will transmit all of the packets in its buffer before permitting the next lower priority to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue will begin transmitting any packets it may have received.

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

Command	Parameters
config bandwidth_control	[<portlist>| all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit <value 64-1024000>]}(1)
show bandwidth_control	{<portlist>}
config scheduling	[<portlist> | all] <class_id 0-7> [strict | weight<value 1-127>]}(1)
config scheduling_mechanism	[<portlist> | all] [strict | wrr]
show scheduling	{<portlist>}
show scheduling_mechanism	{<portlist>}
config 802.1p user_priority	[<portlist> |all] <priority 0-7> <class_id 0-7>
show 802.1p user_priority	{<portlist>}
config 802.1p default_priority	[<portlist> | all] <priority 0-7>
show 802.1p default_priority	{<portlist>}
enable hol_prevention	
disable hol_prevention	
show hol_prevention	
config mgmt_pkt_priority	[default |<priority 0-7>]
show mgmt_pkt_priority	

Each command is listed, in detail, in the following sections.

config bandwidth_control

Purpose	Used to configure bandwidth control on a port by-port basis.
Syntax	**config bandwidth_control [<portlist>| all] {rx_rate [no_limit | <value 64-1024000>] | tx_rate [no_limit <value 64-1024000>]}(1)**
Description	This command is used to configure bandwidth on a port by-port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *rx_rate* – Specifies that one of the parameters below (*no_limit* or <*value 64-1024000*>) will be applied to the rate at which the above specified ports will be allowed to receive packets • *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. • <*value 64-1024000*> – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive. *tx_rate* – Specifies that one of the parameters below (*no_limit* or <*value 64-1024000*>) will be applied to the rate at which the above specified ports will be allowed to transmit packets. • *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. • <*value 64-1024000*> – Specifies the packet limit, in Kbps, that the above ports will be allowed to receive.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure bandwidth control:

```
DGS-3700-12:5#config bandwidth_control 1-10 tx_rate 64
Command: config bandwidth_control 1-10 tx_rate 64

Success.

DGS-3700-12:5#
```

show bandwidth_control

Purpose	Used to display the bandwidth control table.
Syntax	**show bandwidth_control {<portlist>}**
Description	This command is used to display the current bandwidth control configuration on the Switch, on a port-by-port basis.
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed.
Restrictions	None.

Example usage:

To display port bandwidth control table:

```
DGS-3700-12:5#show bandwidth_control 1-10
Command: show bandwidth_control 1-10

Bandwidth Control Table

Port   RX Rate       TX Rate      Effective RX    Effective TX
      (Kbit/sec)    (Kbit/sec)    (Kbit/sec)      (Kbit/sec)
----  ----------    ----------    --------------  ---------------
 1    no_limit      no_limit      no_limit           no_limit
 2    no_limit      no_limit      no_limit           no_limit
 3    no_limit      no_limit      no_limit           no_limit
 4    no_limit      no_limit      no_limit           no_limit
 5    no_limit      no_limit      no_limit           no_limit
 6    no_limit      no_limit      no_limit           no_limit
 7    no_limit      no_limit      no_limit           no_limit
 8    no_limit      no_limit      no_limit           no_limit
 9    no_limit      no_limit      no_limit           no_limit
10    no_limit      no_limit      no_limit           no_limit

DGS-3700-12:5#
```

config scheduling

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling [<portlist> | all] <class_id 0-7> [strict | weight <value 1-127>]}(1)**
Description	The Switch contains eight hardware priority queues. Incoming packets must be mapped to one of these eight queues. This command is used to specify the rotation by which these eight hardware priority queues are emptied. The Switch's default (if the config scheduling command is not used, or if the config scheduling command is entered with *weight* parameters set to 0) is to empty the 8 hardware priority queues in order – from the highest priority queue (hardware queue 7) to the lowest priority queue (hardware queue 0). Each hardware queue will transmit all of the packets in its buffer before allowing the next lower priority queue to transmit its packets. When the lowest hardware priority queue has finished transmitting all of its packets, the highest hardware priority queue can again transmit any packets it may have received. The *weight* parameter allows the user to specify the maximum number of packets a given hardware priority queue can transmit before allowing the next lowest hardware priority queue to begin transmitting its packets. A value between 1 and 127 can be specified. For example, if a value of 3 is specified, then the highest hardware priority queue (number 7) will be allowed to transmit 3 packets – then the next lowest hardware priority queue (number 6) will be allowed to transmit 3 packets, and so on, until all of the queues have transmitted 3 packets. The process will then repeat.
Parameters	*<class_id 0-7>* – This specifies which of the eight hardware priority queues the **config scheduling** command will apply to. The eight hardware priority queues are identified by number – from 0 to 7 – with the 0 queue being the lowest priority. *[<portlist> | all]* – Specifes a range of ports to be configured. *strict* – Specifies this queue is always working in strict mode. *weight <value 1-127>* – Using weighted fair algorithm to handle packets in priority queues. Means each queue will operate based on its setting of max_packet.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each queue:

```
DGS-3700-12:5#config scheduling 10 3 strict
Command: config scheduling 10 3 strict

Success.

DGS-3700-12:5#
```

config scheduling mechanism

Purpose	Used to configure the traffic scheduling mechanism for each COS queue.
Syntax	**config scheduling_mechanism [<portlist> | all] [strict | wrr]**
Description	This command is used to specify how the switch handles packets in priority queues.
Parameters	*<portlist>* – Select the port of list of ports you wish to configure. *all* – Choose this option to select all ports. *strict* – The highest queue first process.That is,the highest queue should be finished at first. *wrr* – Using weighted roundrobin algorithm to handle packets in priority queues.
Restrictions	Only Administrator and Operation-level users can issue this command.

Example usage:

To configure the traffic scheduling mechanism for each COS queue:

```
DGS-3700-12:5#config scheduling_mechanism 1 strict
Command: config scheduling_mechanism 1 strict

Success.

DGS-3700-12:5#
```

show scheduling

Purpose	Used to display the currently configured traffic scheduling on the Switch.
Syntax	**show scheduling {<portlist>}**
Description	This command is used to display the current traffic scheduling parameters in use on the Switch.
Parameters	*<portlist>* – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To display the current scheduling configuration:

```
DGS-3700-12:5#show scheduling 1,2,3
Command: show scheduling 1-3

 QOS Output Scheduling

 Port 1
     Class ID  Weight
     --------  ------
     Class-0   1
     Class-1   2
     Class-2   3
     Class-3   4
     Class-4   5
     Class-5   6
     Class-6   7
     Class-7   8

 Port 2
     Class ID  Weight
     --------  ------
     Class-0   1
     Class-1   2
     Class-2   3
     Class-3   4

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

show scheduling_mechanism

Purpose	Used to show the traffic scheduling mechanism.
Syntax	**show scheduling_mechanism {<portlist>}**
Description	This command is used to display the current traffic scheduling mechanism in use on the Switch.
Parameters	*<portlist>* – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To display the scheduling mechanism:

```
DGS-3700-12:5#show scheduling_mechanism 1-4
Command: show scheduling_mechanism 1-4

 QOS scheduling_mechanism

 Port   Mode
 -----  ------
 1      Strict
 2      Strict
 3      Strict
 4      Strict

DGS-3700-12:5#
```

config 802.1p user_priority

Purpose	Used to map the 802.1p user priority of an incoming packet to one of the eight hardware queues available on the Switch.
Syntax	**config 802.1p user_priority [<portlist> |all] <priority 0-7> <class_id 0-7>**
Description	This command allows users to configure the way the Switch will map an incoming packet, based on its 802.1p user priority, to one of the eight available hardware priority queues on the Switch. The Switch's default is to map the following incoming 802.1p user priority values to the eight hardware priority queues: 802.1p Hardware Queue Remark 0 2 Mid-low 1 0 Lowest 2 1 Lowest 3 3 Mid-low 4 4 Mid-high 5 5 Mid-high 6 6 Mid-high 7 7 Highest This mapping scheme is based upon recommendations contained in IEEE 802.1D. Change this mapping by specifying the 802.1p user priority users want to map to the <*class_id 0-7*> (the number of the hardware queue).
Parameters	*[<portlist> | all]* – Specifes a range of ports to be configured. *All* specifies all ports. <*priority 0-7*> – The 802.1p user priority you want to associate with the <*class_id 0-7*> (the number of the hardware queue) with. <*class_id 0-7*> – The number of the Switch's hardware priority queue. The Switch has eight hardware priority queues available. They are numbered between 0 (the lowest priority) and 7 (the highest priority).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1p user priority on the Switch:

```
DGS-3700-12:5#config 802.1p user_priority 1 1 3
Command: config 802.1p user_priority 1 1 3

Success.

DGS-3700-12:5#
```

show 802.1p user_priority

Purpose	Used to display the current mapping between an incoming packet's 802.1p priority value and one of the Switch's eight hardware priority queues.
Syntax	**show 802.1p user_priority {<portlist>}**
Description	This command is used to display the current mapping of an incoming packet's 802.1p priority value to one of the Switch's eight hardware priority queues.
Parameters	*{<portlist>}* – Specifies a range of ports to be displayed.
Restrictions	None.

Example usage:

To show 802.1p user priority:

```
DGS-3700-12:5#show 802.1p user_priority 1-2
Command: show 802.1p user_priority 1-2

 QOS Class of Traffic

 Port 1
     Priority-0  ->  <Class-2>
     Priority-1  ->  <Class-0>
     Priority-2  ->  <Class-1>
     Priority-3  ->  <Class-3>
     Priority-4  ->  <Class-4>
     Priority-5  ->  <Class-5>
     Priority-6  ->  <Class-6>
     Priority-7  ->  <Class-7>

 Port 2
     Priority-0  ->  <Class-2>
     Priority-1  ->  <Class-0>
     Priority-2  ->  <Class-1>
     Priority-3  ->  <Class-3>
     Priority-4  ->  <Class-4>
     Priority-5  ->  <Class-5>
     Priority-6  ->  <Class-6>
     Priority-7  ->  <Class-7>

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

config 802.1p default_priority

Purpose	Used to configure the 802.1p default priority settings on the Switch. If an untagged packet is received by the Switch, the priority configured with this command will be written to the packet's priority field.
Syntax	**config 802.1p default_priority [<portlist> | all] <priority 0-7>**
Description	This command allows the user to specify default priority handling of untagged packets received by the Switch. The priority value entered with this command will be used to determine which of the eight hardware priority queues the packet is forwarded to.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured. *all* – Specifies that the command applies to all ports on the Switch. *<priority 0-7>* – The priority value to assign to untagged packets received by the Switch or a range of ports on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1p default priority on the Switch:

```
DGS-3700-12:5#config 802.1p default_priority all 5
Command: config 802.1p default_priority all 5

Success.

DGS-3700-12:5#
```

show 802.1 default_priority

Purpose	Used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Syntax	**show 802.1p default_priority {<portlist>}**
Description	This command is used to display the currently configured 802.1p priority value that will be assigned to an incoming, untagged packet before being forwarded to its destination.
Parameters	*<portlist>* – Specifies a port or range of ports to be configured.
Restrictions	None.

Example usage:

To display the current 802.1p default priority configuration on the Switch:

```
DGS-3700-12:5#show 802.1p default_priority
Command: show 802.1p default_priority

Port         Priority         Effective Priority
----         -----------      ------------------
1              0                      0
2              0                      0
3              0                      0
4              0                      0
5              0                      0
6              0                      0
7              0                      0
8              0                      0
9              0                      0
10             0                      0
11             0                      0
12             0                      0

DGS-3700-12:5#
```

enable hol_prevention

Purpose	Used to enable the HOL prevention state.
Syntax	**enable hol_prevention**
Description	This command enables the HOL prevention function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable HOL prevention:

```
DGS-3700-12:5#enable hol_prevention
Command: enable hol_prevention

Success.
DGS-3700-12:5#
```

disable hol_prevention

Purpose	Used to disable HOL prevention.
Syntax	**disable hol_prevention**
Description	This command disables the HOL prevention function on the switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable HOL prevention:

```
DGS-3700-12:5#disable hol_prevention
Command: disable hol_prevention

Success.
DGS-3700-12:5#
```

show hol_prevention

Purpose	Used to show the HOL prevention state.
Syntax	**show hol_prevention**
Description	This command displays the HOL prevention state.
Parameters	None.
Restrictions	None.

Example usage:

To display HOL prevention:

```
DGS-3700-12:5#show hol_prevention
Command: show hol_prevention

Device HOL Prevention State: Enabled

DGS-3700-12:5#
```

config mgmt_pkt_priority

Purpose	Used to configure the priority of managment packet.
Syntax	**config mgmt_pkt_priority [default |<priority 0-7>]**
Description	This command is used to configure the priority of managment packet.
Parameters	*default*– Specifies to use the original management packet priority. <*priority 0-7*> - Specifes the priority of packets, the range is *0-7*. 7 is highest priority.
Restrictions	Only Administrator level users can issue this command.

Example usage:

To config priority of managment packet setting:

```
DGS-3700-12:5#config mgmt_pkt_priority 3
Command: config mgmt_pkt_priority 3

Success.

DGS-3700-12:5#
```

show mgmt_pkt_priority

Purpose	Used to display current priority of management packet.
Syntax	**show mgmt_pkt_priority**
Description	This command is used to display current priority of management packet.
Parameters	None.
Restrictions	None.

Example usage:

To display the current priority of management packets:

```
DGS-3700-12:5# show mgmt_pkt_priority
Command: show mgmt_pkt_priority

Management Packet Priority:3

DGS-3700-12:5#
```

44

TRAFFIC CONTROL COMMANDS

On a computer network, packets such as Multicast packets and Broadcast packets continually flood the network as normal procedure. At times, this traffic may increase do to a malicious endstation on the network or a malfunctioning device, such as a faulty network card. Thus, switch throughput problems will arise and consequently affect the overall performance of the switch network. To help rectify this packet storm, the Switch will monitor and control the situation.

The packet storm is monitored to determine if too many packets are flooding the network, based on the threshold level provided by the user. Once a packet storm has been detected, the Switch will drop packets coming into the Switch until the storm has subsided. This method can be utilized by selecting the **Drop** option of the **Action** field in the window below.

The Switch will also scan and monitor packets coming into the Switch by monitoring the Switch's chip counter. This method is only viable for Broadcast and Multicast storms because the chip only has counters for these two types of packets. Once a storm has been detected (that is, once the packet threshold set below has been exceeded), the Switch will shutdown the port to all incoming traffic with the exception of STP BPDU packets, for a time period specified using the *countdown* field. If this field times out and the packet storm continues, the port will be placed in a Shutdown Forever mode which will produce a warning message to be sent to the Trap Receiver. Once in Shutdown Forever mode, one method of recovering this port is to manually recoup it using the **Port Configuration** window in the **Administration** folder and selecting the disabled port and returning it to an Enabled status. To utilize this method of Storm Control, choose the **Shutdown** option of the **Action** field in the window below.

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

Command	Parameters
config traffic control	[<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <value 5-30> | countdown [value 0 | <value 5-30>]}(1)
show traffic control	{<portlist>}
config traffic trap	[none | storm_occurred | storm_cleared | both]

Each command is listed, in detail, in the following sections.

config traffic control

Purpose	Used to configure broadcast/multicast/unicast packet storm control. The software mechanism is provided to monitor the traffic rate in addition to the hardware storm control mechanism previously provided.
Syntax	**config traffic control [<portlist> | all] {broadcast [enable | disable] | multicast [enable | disable] | unicast [enable | disable] | action [drop | shutdown] | threshold <value 0-255000> | time_interval <value 5-30> | countdown [value 0 | <value 5-30>]}(1)**
Description	This command is used to configure broadcast/multicast/unicast storm control. By adding the new software traffic control mechanism, the user can now use both a hardware and software mechanism, the latter of which will now provide shutdown, recovery and trap notification functions for the Switch.
Parameters	*<portlist>* – Used to specify a group list of ports to be configured for traffic control, as defined below: *all* – Specifies all portlists are to be configured for traffic control on the Switch. *broadcast [enable | disable]* – Enables or disables broadcast storm control. *multicast [enable | disable]* – Enables or disables multicast storm control. *unicast [enable | disable]* – Enables or disables unicast traffic control. *action* – Used to configure the action taken when a storm control has been detected on the Switch. The user has two options: • *drop* – Utilizes the hardware Traffic Control mechanism, which means the Switch's hardware will determine the Packet Storm based on the Threshold value stated and drop packets until the issue is resolved. • *shutdown* – Utilizes the Switch's software Traffic Control mechanism to determine

config traffic control

	the Packet Storm occurring. Once detected, the port will deny all incoming traffic to the port except STP BPDU packets, which are essential in keeping the Spanning Tree operational on the Switch. If the countdown timer has expired and yet the Packet Storm continues, the port will be placed in Shutdown Forever mode and is no longer operational until the user manually resets the port using the **config ports enable** command. Choosing this option obligates the user to configure the *time_interval* field as well, which will provide packet count samplings from the Switch's chip to determine if a Packet Storm is occurring. *threshold* <*value 0-255000*> – The upper threshold at which the specified traffic control is switched on. The <*value*> is the number of broadcast/multicast/unicast packets, in packets per second (pps), received by the Switch that will trigger the storm traffic control measures. The default setting is *131072*. *time_interval* – The Interval will set the time between Multicast and Broadcast packet counts sent from the Switch's chip to the Traffic Control function. These packet counts are the determining factor in deciding when incoming packets exceed the Threshold value. *value 5-30* – The Interval may be set between *5* and *30* seconds with the default setting of 5 seconds. *countdown* – The countdown timer is set to determine the amount of time, in minutes, that the Switch will wait before shutting down the port that is experiencing a traffic storm. The switch will shutdown the port only if the traffic level exceeds the configured threshold all the time during this countdown period. This parameter is only useful for ports configured as **shutdown** in the **action** field of this command and therefore will not operate for Hardware based Traffic Control implementations. • *value 0* – 0 is the default setting for this field and *0* will denote that the port will never shutdown forever. • *value 5-30* – Select a time from *5* to *30* minutes that the Switch will wait before shutting down. Once this time expires and the port is still experiencing packet storms, the port will be placed in shutdown forever mode and can only be manually recovered using the config ports command mentioned previously in this manual.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure traffic control and enable broadcast storm control for ports 1-12:

```
DGS-3700-12:5#config traffic control 1-12 broadcast enable action shutdown threshold 1
countdown 10 time_interval 10
Command: config traffic control 1-12 broadcast enable action shutdown threshold 1
countdown 10 time_interval 10

Success.

DGS-3700-12:5#
```

show traffic control

Purpose	Used to display current traffic control settings.
Syntax	**show traffic control { <portlist> }**
Description	This command displays the current storm traffic control configuration on the Switch.
Parameters	<*portlist*> – Used to specify port or list of ports for which to display traffic control settings. The beginning and end of the port list range are separated by a dash.
Restrictions	None.

Example usage:

To display traffic control settings:

```
DGS-3700-12:5#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    131072 Disabled  Disabled  Disabled drop     0         5
2    131072 Disabled  Disabled  Disabled drop     0         5
3    131072 Disabled  Disabled  Disabled drop     0         5
4    131072 Disabled  Disabled  Disabled drop     0         5
5    131072 Disabled  Disabled  Disabled drop     0         5
6    131072 Disabled  Disabled  Disabled drop     0         5
7    131072 Disabled  Disabled  Disabled drop     0         5
8    131072 Disabled  Disabled  Disabled drop     0         5
9    131072 Disabled  Disabled  Disabled drop     0         5
10   131072 Disabled  Disabled  Disabled drop     0         5
11   131072 Disabled  Disabled  Disabled drop     0         5
12   131072 Disabled  Disabled  Disabled drop     0         5

Note: For unicast storm traffic, the violated action is always 'drop'.
DGS-3700-12:5#
```

config traffic trap

Purpose	Used to configure the trap settings for the packet storm control mechanism.
Syntax	**config traffic trap [none | storm_occurred | storm_cleared | both]**
Description	This command will configure how packet storm control trap messages will be used when a packet storm is detected by the Switch. This function can only be used for the software traffic storm control mechanism (when the **action** field in the **config traffic storm_control** command is set as **shutdown**).
Parameters	*none* – No notification will be generated or sent when a packet storm control is detected by the Switch. *storm _occurred* – A notification will be generated and sent when a packet storm has been detected by the Switch. *storm_cleared* – A notification will be generated and sent when a packet storm has been cleared by the Switch. *both* – A notification will be generated and sent when a packet storm has been detected and cleared by the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure notifications to be sent when a packet storm control has been detected and cleared by the Switch.

```
DGS-3700-12:5# config traffic trap both
Command: config traffic trap both

Success.

DGS-3700-12:5#
```

45

SIMPLE RED COMMANDS

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

Command	Parameters
enable sred	
disable sred	
config sred	[<portlist>|all] [<class_id 0-7>|all] { threshold {low <value 0-100>|high<value 0-100>}(1)| drop_rate {low<value 1-8>|high<value 1-8>}(1)| drop_green [enable|disable]}(1)
show sred	{ <portlist>{ <class_id 0-7>}}
show sred drop_counter	{<portlist>}
config dscp trust	[<portlist>|all] state [enable|disable]
show dscp trust	{<portlist>}
config dscp map	[<portlist>|all] [dscp_priority <dscp_list> to <priority 0-7>| dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green|red|yellow]]
show dscp map	{ <portlist> } [dscp_priotity | dscp_dscp | dscp_color] {dscp <dscp_list>}
config 802.1p map	[<portlist>|all] 1p_color [<priority_list] to [green|red |yellow]
show 802.1p map 1p_color	{ <portlist>}

Each command is listed, in detail, in the following sections.

enable sred

Purpose	Used to enable the simple RED function.
Syntax	**enable sred**
Description	This command is used to enable the sRED function. By default, sRED is disabled.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable sred:

```
DGS-3700-12:5#enable sred
Command: enable sred

Success.

DGS-3700-12:5#
```

disable sred

Purpose	Used to disable the simple RED function.
Syntax	**disable sred**
Description	This command is used to disable the sRED function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable sred:

```
DGS-3700-12:5#disable sred
Command: disable sred

Success.

DGS-3700-12:5#
```

config sred

Purpose	Used to config the simple RED parameter.
Syntax	**config sred [<portlist>|all] [<class_id 0-7>|all]** **{ threshold {low <value 0-100>|high<value 0-100>}(1)|** **drop_rate {low<value 1-8>|high<value 1-8>}(1)|** **drop_green [enable|disable]}(1)**
Description	This command is used to configure sRED threshold per port or per port per queue.
Parameters	*portlist* – A range of ports to config. *class_id* – This specifies which of the 8 hardware CoS queues the config sred command will apply to. *threshold* – **low** – low threshold that Specifies the percent of space utilized. By default, the value is 60. The range is 0 to 100. **high** – high threshold that Specifies the percent of queue space utilized. By default, the value is 80. The range is 0 to 100. *drop_rate* – **low** – probabilistic drop rate if above the low threshold, By default, the value is 1. **high** – probabilistic drop rate if above the high threshold. By default, the value is 1. *drop_green* – **disable** – probabilistic drop red colored packets if the queue depth is above the low threshold, and probabilistic drop yellow colored packets if the queue depth is above the high threshold. By default, if the option is not specified, the setting is disabled. **enable** – probabilistic drop yellow and red colored packets if the queue depth is above the low threshold, and probabilistic drop green colored packets if the queue depth is above the high threshold.  **NOTE:** There are 8 drop rates: 1 100% 2 6.25% 3 3.125% 4 1.5625% 5 0.78125% 6 0.390625% 7 0.1953125% 8 0.09765625%
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure sred:

```
DGS-3700-12:5# config sred all all threshold low 64 high 80 drop_rate low 8 high 8
drop_green disable
Command: config sred all all threshold low 64 high 80 drop_rate low 8 high 8
drop_green disable

Success.

DGS-3700-12:5#
```

show sred

Purpose	Used to display the simple RED configure parameter.
Syntax	**show sred { <portlist>{ <class_id 0-7>}}**
Description	This command is used to display the current threshold(per port and per queue) parameters in use on the switch
Parameters	*portlist* – A range of ports to show. *class_id* – This specifies which of the hardware CoS queues the config sred command will apply to.
Restrictions	None.

Example usage:

To show sred:

```
DGS-3700-12:5#show sred
Command: show sred

Simple RED Globale Status: Disabled

Port Class Drop Green Threshold Drop Rate
                      Low  High Low  High
---- -----  --------- ---- ---- ---- ----
1    0      Disabled  60   80   1    1
1    1      Disabled  60   80   1    1
1    2      Disabled  60   80   1    1
1    3      Disabled  60   80   1    1
1    4      Disabled  60   80   1    1
1    5      Disabled  60   80   1    1
1    6      Disabled  60   80   1    1
1    7      Disabled  60   80   1    1
2    0      Disabled  60   80   1    1
2    1      Disabled  60   80   1    1
2    2      Disabled  60   80   1    1
2    3      Disabled  60   80   1    1
2    4      Disabled  60   80   1    1
2    5      Disabled  60   80   1    1
2    6      Disabled  60   80   1    1
2    7      Disabled  60   80   1    1
3    0      Disabled  60   80   1    1

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

show sred drop_counter

Purpose	Used to display the simple RED drop packet counter per port.
Syntax	**show sred drop_counter {<portlist>}**
Description	This command is used to display, for the egress port, the count of dropped packets
Parameters	*portlist* – A range of ports to show.
Restrictions	None.

Example usage:

This example displays red and yellow packet drop counts for all ports:

```
DGS-3700-12:5#show sred drop_counter
Command: show sred drop_counter

Port  Yellow          Red
----  --------------  --------------
1     0               0
2     0               0
3     0               0
4     0               0
5     0               0
6     0               0
7     0               0
8     0               0
9     0               0
10    0               0
11    0               0
12    0               0

DGS-3700-12:5#
```

config dscp trust

Purpose	Enable/Disable DSCP trust state on selected portlist.
Syntax	**config dscp trust [<portlist>|all] state [enable|disable]**
Description	This command is used to onfigure the port DSCP trust state. When DSCP is not trusted, 1p is trusted.
Parameters	*portlist* – A range of ports to config. *state* – Enable/disable to trust DSCP. By default, DSCP trust is disabled.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This config DSCP trust:

```
DGS-3700-12:5#config dscp trust 1-8 state enable
Command: config dscp trust 1-8 state enable

Success.

DGS-3700-12:5#
```

show dscp trust

Purpose	Used to display DSCP trust state.
Syntax	**show dscp trust {<portlist>}**
Description	This command is used to display DSCP trsut state.
Parameters	*portlist* – A range of ports to display.
Restrictions	None.

Example usage:

To display the DSCP trust state:

```
DGS-3700-12:5#show dscp trust
Command: show dscp trust

Port    DSCP-Trust
-----   -----------
1        Disabled
2        Disabled
3        Disabled
4        Disabled
5        Enabled
6        Enabled
7        Enabled
8        Enabled
9        Disabled
10       Disabled
11       Disabled
12       Disabled

DGS-3700-12:5#
```

config dscp map

Purpose	config mapping of DSCP to priority and packet's initial color .
Syntax	**config dscp map [<portlist>|all] [dscp_priority <dscp_list> to <priority 0-7>| dscp_dscp <dscp_list> to <dscp 0-63> | dscp_color <dscp_list> to [green|red|yellow]]**
Description	The mapping of DSCP to COS will be used to determine the priority of the packet (which will be then used to determine the scheduling queue) when the port is in DSCP trust state. The mapping of DSCP to color will be used to determine the initial color of the packet when the policing function of the packet is color aware and the packet is DSCP-trusted. The DSCP-to-DSCP mapping is used in the swap of DSCP of the packet when the packet is ingressed to the port. The remaining processing of the packet will be based on the new DSCP. By default, the DSCP is mapped to the same DSCP.
Parameters	*portlist* – Specifies ports to be configured. *dscp_priority* – Specifies a list of DSCP value to be mapped to a specific priority *priority* – Specifies the result priority of mapping. The default mapping are:

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
priority	0	1	2	3	4	5	6	7

	dscp_dscp – Specifies a list of DSCP value to be mapped to a specific dscp. *dscp* – Specifies the result DSCP of mapping. *dscp_color* – Specifies a list of DSCP value to be mapped to a specific color. *color* – Specifies the result color of mapping.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This config DSCP map:

```
DGS-3700-12:5#config dscp map 1-8 dscp_priority 1 to 1
Command: config dscp map 1-8 dscp_priority 1 to 1

Success.

DGS-3700-12:5#
```

show dscp map

Purpose	Used to display the DSCP map configure parameter.
Syntax	**show dscp map { <portlist> } [dscp_priotity | dscp_dscp | dscp_color] {dscp <dscp_list>}**
Description	This command is used to show DSCP trusted portlist and mapped color, priority and DSCP.
Parameters	*portlist* – Specifies a range of ports to display. *dscp* – Specifies DSCP value that will be mapped.
Restrictions	None.

Example usage:

This show DSCP map:

```
DGS-3700-12:5#show dscp map dscp_color
Command: show dscp map dscp_color

DSCP to Color Mapping:
Port 1
         DSCP 0-63 is mapped to Green
Port 2
         DSCP 0-63 is mapped to Green
Port 3
         DSCP 0-63 is mapped to Green
Port 4
         DSCP 0-63 is mapped to Green
Port 5
         DSCP 0-63 is mapped to Green
Port 6
         DSCP 0-63 is mapped to Green
Port 7
         DSCP 0-63 is mapped to Green
Port 8
         DSCP 0-63 is mapped to Green
Port 9
         DSCP 0-63 is mapped to Green
Port 10
         DSCP 0-63 is mapped to Green
CTRL+C ESC q Quit SPACE n Next Page ENTER Next Entry a All
```

config 802.1p map

Purpose	Config mapping of 802.1p to packet's initial color.
Syntax	**config 802.1p map [<portlist>|all] 1p_color [<priority_list] to [green|red |yellow]**
Description	This command is used to configure mapping of 802.1p to packet's initial color. The mapping of 802.1p to color will be used to determine the initial color of the packet, when the policing function of the packet is color aware and the packet is 802.1p-trusted.
Parameters	*portlist* – A range of ports to configure. *priority* – Source priority of incoming packets. *color* – Mapped color for packet, default value is green
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

This config 802.1p map:

```
DGS-3700-12:5#config 802.1p map 1-8 1p_color 1 to red
Command: config 802.1p map 1-8 1p_color 1 to red
Success.

DGS-3700-12:5#
```

show 802.1p map

Purpose	Used to display the 802.1p to color mapping
Syntax	**show 802.1p map 1p_color { <portlist>}**
Description	This command is used to display the 802.1p to color mapping
Parameters	*portlist* – A range of ports to show.
Restrictions	None.

Example usage:

This show 802.1p map:

```
DGS-3700-12:5#show 802.1p map 1p_color
Command: show 802.1p map 1p_color

802.1p to Color Mapping:
-------------------------------------------------------------
Port 0      1      2      3      4      5      6      7
---- ------ ------ ------ ------ ------ ------ ------ ------
1    Green  Red    Green  Green  Green  Green  Green  Green
2    Green  Red    Green  Green  Green  Green  Green  Green
3    Green  Red    Green  Green  Green  Green  Green  Green
4    Green  Red    Green  Green  Green  Green  Green  Green
5    Green  Red    Green  Green  Green  Green  Green  Green
6    Green  Red    Green  Green  Green  Green  Green  Green
7    Green  Red    Green  Green  Green  Green  Green  Green
8    Green  Red    Green  Green  Green  Green  Green  Green
9    Green  Green  Green  Green  Green  Green  Green  Green
10   Green  Green  Green  Green  Green  Green  Green  Green
11   Green  Green  Green  Green  Green  Green  Green  Green
12   Green  Green  Green  Green  Green  Green  Green  Green

DGS-3700-12:5#
```

46

SAFEGUARD ENGINE COMMANDS

Periodically, malicious hosts on the network will attack the Switch by utilizing packet flooding (ARP Storm) or other methods. These attacks may increase the CPU utilization beyond its capability. To alleviate this problem, the Safeguard Engine function was added to the Switch's software.

The Safeguard Engine can help the overall operability of the Switch by minimizing the workload of the Switch while the attack is ongoing, thus making it capable to forward essential packets over its network in a limited bandwidth. When the Switch either (a) receives too many packets to process or (b) exerts too much memory, it will enter an **Exhausted** mode. When in this mode, the Switch will perform the following tasks to minimize the CPU usage:

a. It will limit bandwidth of receiving ARP packets.
b. It will limit the bandwidth of IP packets received by the Switch.

IP packets may also be limited by the Switch by configuring only certain IP addresses to be accepted. This method can be accomplished through the CPU Interface Filtering mechanism explained in the previous section. Once the user configures these acceptable IP addresses, other packets containing different IP addresses will be dropped by the Switch, thus limiting the bandwidth of IP packets. To keep the process moving fast, be sure not to add many conditions on which to accept these acceptable IP addresses and their packets, this limiting the CPU utilization.

Once in Exhausted mode, the packet flow will decrease by half of the level that caused the Switch to enter Exhausted mode. After the packet flow has stabilized, the rate will initially increase by 25% and then return to a normal packet flow.

NOTICE: When the Safeguard Engine is enabled, the Switch will allot bandwidth to various traffic flows (ARP, IP) using the FFP (Fast Filter Processor) metering table to control the CPU utilization and limit traffic. This may limit the speed of routing traffic over the network.

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

Command	Parameters
config safeguard_engine	{ state [enable|disable] |utilization { rising <value 20-100> | falling <value 20-100>}(1) | trap_log [enable|disable] | mode [strict | fuzzy]}(1)
show safeguard_engine	

Each command is listed, in detail, in the following sections.

config safeguard_engine

Purpose	To configure ARP storm control for system.
Syntax	**config safeguard_engine { state [enable|disable] |utilization { rising <value 20-100> | falling <value 20-100>}(1) | trap_log [enable|disable] | mode [strict | fuzzy]}(1)**
Description	This command is used to configure Safeguard Engine to minimize the effects of an ARP storm.
Parameters	*state [enable | disable]* – Select the running state of the Safeguard Engine function as enable or disable. *utilization* – Select this option to trigger the Safeguard Engine function to enable based on the following determinates: *rising <value 20-100>* – The user can set a percentage value of the rising CPU utilization which will trigger the Safeguard Engine function. Once the CPU utilization rises to this percentage, the Safeguard Engine mechanism will initiate. *falling <value 20-100>* – The user can set a percentage value of the falling CPU utilization which will trigger the Safeguard Engine function to cease. Once the CPU utilization falls to this percentage, the Safeguard Engine mechanism will shut down. *trap_log [enable | disable]* – Choose whether to enable or disable the sending of messages to the device's SNMP agent and switch log once the Safeguard Engine has been activated by a high CPU utilization rate. *mode [strict | fuzzy]* – Used to select the type of Safeguard Engine to be activated by the Switch when the CPU utilization reaches a high rate. The user may select:

config safeguard_engine

	strict – If selected, this function will instruct the Switch to minimize the IP and ARP traffic flow to the CPU by dynamically allotting an even bandwidth to all traffic flows. *fuzzy* – If selected, this function will stop accepting all ARP packets not intended for the Switch, and will stop receiving all unnecessary broadcast IP packets, until the storm has subsided.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the safeguard engine for the Switch:

```
DGS-3700-12:5#config safeguard_engine state enable utilization rising 45
Command: config safeguard_engine state enable utilization rising 45

Success.

DGS-3700-12:5#
```

show safeguard_engine

Purpose	Used to display current Safeguard Engine settings.
Syntax	**show safeguard_engine**
Description	This command is used to list the current status and type of the Safeguard Engine settings currently configured.
Parameters	None.
Restrictions	None.

Example usage:

To display the safeguard engine status:

```
DGS-3700-12:5#show safeguard_engine
Command: show safeguard_engine

Safeguard Engine State           :  Disabled
Safeguard Engine Current Status  :  Normal Mode
=====================================================
CPU Utilization Information:
Rising Threshold  :  30%
Falling Threshold :  20%
Trap/Log State    :  Enabled
Mode              :  Strict

DGS-3700-12:5#
```

47

IP-MAC BINDING

The IP network layer uses a four-byte address. The Ethernet link layer uses a six-byte MAC address. Binding these two address types together allows the transmission of data between the layers. The primary purpose of IP-MAC binding is to restrict the access to a switch to a number of authorized users. Only the authorized client can access the Switch's port by checking the pair of IP-MAC addresses with the pre-configured database. If an unauthorized user tries to access an IP-MAC binding enabled port, the system will block the access by dropping its packet. The maximum number of IP-MAC binding entries is dependant on chip capability (e.g. the ARP table size) and storage size of the device. For the DGS-3700 Series, the maximum number of IP-MAC Binding entries is 511. The creation of authorized users can be manually configured by CLI or Web. The function is port-based, meaning a user can enable or disable the function on the individual port.

ACL Mode

Due to some special cases that have arisen with the IP-MAC binding, this Switch has been equipped with a special ACL Mode for IP-MAC Binding, which should alleviate this problem for users. When enabled, the Switch will create two entries in the Access Profile Table. The entries may only be created if there are at least two Profile IDs available on the Switch. If not, when the ACL Mode is enabled, an error message will be prompted to the user. When the ACL Mode is enabled, the Switch will only accept packets from a created entry in the IP-MAC Binding Setting window. All others will be discarded.

To configure the ACL mode, the user must first create an IP-MAC binding using the **create address_binding ip_mac ipaddress** command and select the mode as *acl*. Then the user must enable the mode by entering the **enable address_binding acl_mode** command. If an IP-MAC binding entry is created and the user wishes to change it to an ACL mode entry, the user may use the **config address_binding ip_mac ipaddress** command and select the mode as *acl*.

NOTE: When configuring the ACL mode function of the IP-MAC binding function, please pay close attention to previously set ACL entries. Since the ACL mode entries will fill the first two available access profiles and access profile IDs denote the ACL priority, the ACL mode entries may take precedence over other configured ACL entries. This may render some user-defined ACL parameters inoperable due to the overlapping of settings combined with the ACL entry priority (defined by profile ID). For more information on ACL settings, please see "Configuring the Access Profile" section mentioned previously in this chapter.

NOTE: Once ACL profiles have been created by the Switch through the IP-MAC binding function, the user cannot modify, delete or add ACL rules to these ACL mode access profile entries. Any attempt to modify, delete or add ACL rules will result in a configuration error as seen in the previous figure.

NOTE: When downloading configuration files to the Switch, be aware of the ACL configurations loaded, as compared to the ACL mode access profile entries set by this function, which may cause both access profile types to experience problems.

The IP-MAC Binding commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
config address_binding ip_mac ports	[<portlist> | all] {state [enable {[strict | loose]} | disable] |allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}(1)
create address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> { ports [<portlist> | all] | mode [arp | acl] }
delete address_binding	[ip_mac [ipaddress <ipaddr> mac_address <macaddr> |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]
config address_binding ip_mac ipaddress	<ipaddr> mac_address <macaddr> { ports [<portlist> | all] | mode [arp | acl]}
show address_binding	{[ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]|blocked [all | vlan_name <vlan_name> mac_address <macaddr>]|ports]}
enable address_binding acl_mode	
disable address_binding acl_mode	
enable address_binding dhcp_snoop	
disable address_binding dhcp_snoop	
clear address_binding dhcp_snoop binding_entry ports	[<portlist>|all]
show address_binding dhcp_snoop	{[max_entry { ports <portlist>} | binding_entry {port <port>}]}
config address_binding dhcp_snoop max_entry ports	[<portlist> | all] limit [<value 1-50> | no_limit]
enable address_binding trap_log	
disable address_binding trap_log	

Each command is listed, in detail, in the following sections.

config address_binding ip_mac ports

Purpose	The config address_binding ip_mac ports command is used to configure per port state of IP-MAC binding in the switch.
Syntax	**config address_binding ip_mac ports[<portlist> | all] {state [enable {[strict | loose]} | disable] | allow_zeroip [enable | disable] | forward_dhcppkt [enable | disable]}(1)**
Description	This command is used to configure per port state of IP-MAC binding on the switch. If a port has been configured as a group member of an aggregagted link, then it can not enable its ip mac binding function. When the binding check state is enabled, for IP packet and ARP packet received by this port, the switch will check whether the IP address and MAC address match the binding entries, the packet will be dropped if they did not match. For this function, the switch can operate in ACL mode or ARP mode, In ARP mode, only ARP packets are checked for binding, In ACL mode, both ARP packet and IP packets are checked for binding. Therefore, ACL mode provides more strict checks for packets. The configrution of an entry in the ACL mode will consume the resources in the switch controller. An ACL mode entry may not be effective. The status of the entry will display this information. When an entry in not effective, the check for IP packet will not be performed.

config address_binding ip_mac ports

	The check for the ARP packet will still be performed. For the check of ARP packet, both of the ARP request and reply packet will be checked. The packet with source IP address not defined in the source-validity binding entry or with source MAC address not defined in the source-validity binding entry, or if the source IP address and source MAC address do not match the pair defined the source-validity binding entry will be dropped. The ARL entry corresponds to source MAC address in the invalid packet so it will be set to a blocked state. When an ARL entry is set to a blocked state, if correct source IP address occurred with the blocked MAC address, the ARL entry for this MAC address will be recovered. If acl_mode is changed, the switch will add/delete ACL access entries automatically when the configured state is enable/disable. (To deny all ip packets on this port). If the acl pool is full and the switch can not create any new ACL access entry, the switch will show a warning message. At this moment, this port will enter normal address_binding mode.
Parameters	*state* – configure address binding port state to enable or disable. When the state is enabled, the port will perform the binding check. *strict* – This mode provides a more strict way of control. If user chooses it, all packets will be sent to CPU, thus all packets will not be forwarded by the hardward until the S/W learn entries for the port. The port will check ARP packets and IP packets by IP-MAC-PORT Binding entries. The packet is found by the entry, the MAC will be set to dynamic. The packet isn't found by the entry, the MAC will be set to block. Other packets will be dropped. The default mode is strict if not specified. *loose* – This mode provides a more loose way of control. If user chooses loose, ARP packets and IP Broadcast packets will go to the CPU. The packet will still be forwarded by the hardware until a specific source MAC is blocked by the software. The port will check ARP packets and IP Broadcast packets by IP-MAC-PORT Binding entries. The packet is found by the entry, the MAC will be set to dynamic. The packet isn't found by the entry, the MAC will be set to block. Other packets will be bypassed. *allow_zeroip* – Specify whether to allow ARP packet with SIP address 0.0.0.0. Supposed that 0.0.0.0 is not configured in the binding list, when it is set to enabled, the ARP packet with this source IP address 0.0.0.0 is allowed; when it is set to disable the ARP packet with this source IP address 0.0.0.0 is dropped. This option does not affect the IP-MAC-Port binding ACL Mode. *forward_dhcppkt* – By default, the dhcp packet with broadcast DA will be flooded. When set to disabled, the broadcast DHCP packet received by the specified port will not be forwarded. This setting is effective when DHCP snooping is enabled, under which case the DHCP packet which has been trapped to CPU needs to be forwarded by the software. This setting controls the forwarding behaviour under this situation. *<portlist>* – Specifies a port or range of ports. *all* – specifies all ports on the switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port 1 enable address_binding:

```
DGS-3700-12:5# config address_binding ip_mac ports 1 state enable
Command: config address_binding ip_mac ports 1 state enable

Success.

DGS-3700-12:5#
```

create address_binding ip_mac ipaddress

Purpose	To create an address_binding entry.
Syntax	**create address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> { ports [<portlist> | all] | mode [arp | acl]}**
Description	This command is used to create an address binding entry. One MAC address can map to multiple ip address If acl mode is enable, the switch will add the according ACL access entries automatically. If user do not choose acl mode or arp mode, default is arp mode.
Parameters	*<ipaddr>* – The IP address of the device where the IP-MAC binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC binding is made. *<ports>* – Specifies a port or range of ports to be configured for address binding. *all* – Specifies that all ports on the switch will be configured for address binding. *mode* – The user may set the mode for this IP-MAC binding settings by choosing one of the following: *arp* – This entry is specified as an arp mode entry. this entry will not be added as access entries. If not specified, the mode is default to ARP mode. If the system is in ARP mode, the arp mode entries and acl mode entries will be effective. If the system is in acl mode, only the acl mode entries will be active. *acl* – This entry is specified as an acl mode entry. If user enable acl mode, this entry will be added as access entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create address binding with arp mode for all ports on the Switch:

```
DGS-3700-12:5#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-11

Success.

DGS-3700-12:5#
```

To create address binding on the Switch to port 1:

```
DGS-3700-12:5#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-
00-00-11 ports 1
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-
00-11 ports 1

Success.

DGS-3700-12:5#
```

To create address binding on the Switch to port 1 and by ACL mode:

```
DGS-3700-12:5#create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 ports 1 mode acl
Command: create address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 ports 1 mode acl

Success.

DGS-3700-12:5#
```

delete address_binding

Purpose	To delete a address binding entry.
Syntax	**delete address_binding [ip_mac [ipaddress <ipaddr> mac_address <macaddr> |all] | blocked [all | vlan_name <vlan_name> mac_address <macaddr>]]**
Description	This command is used to delete an address binding entry. If acl mode is enabled, the switch will delete the according ACL access entries automatically.
Parameters	*ip_mac* – The database that user create for address binding. *blocked* – The address database that system auto learned and blocked. *ipaddr* – The IP address. *macaddr* – The MAC address. *vlan_name* – VLAN name (the blocked MAC belongs to).
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete address binding on the Switch:

```
DGS-3700-12:5# delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: delete address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3700-12:5#
```

config address_binding ip_mac ipaddress

Purpose	To update a address_binding entry.
Syntax	**config address_binding ip_mac ipaddress <ipaddr> mac_address <macaddr> { ports [<portlist> | all] mode [acl | arp]}**
Description	This command is used to update an address binding entry.
Parameters	*<ipaddr>* – The IP address of the device where the IP-MAC binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC binding is made. *ports* – Specifies a port or range of ports to be configured for address binding, if no ports are specified it will apply to all ports. *arp* – This entry is specified as an arp mode entry. this entry will not be added as access entries. If not specified, the mode is default to ARP mode. If the system is in ARP mode, the arp mode entries and acl mode entries will be effective. If the system is in acl mode, only the ACL mode entries will be active; the arp mode entry will no in-effective. *acl* – This entry is specified as an ACL mode entry. If a user enables ACL mode, this entry will be added as an access entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure address_binding with arp mode for all ports on the Switch:

```
DGS-3700-12:5#config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11

Success.

DGS-3700-12:5#
```

To configure address_binding on the Switch to port 1:

```
DGS-3700-12:5#config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 ports 1
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 ports 1

Success.

DGS-3700-12:5#
```

To configure address_binding on the Switch to port 1 and by acl mode:

```
DGS-3700-12:5#config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 ports 1 mode acl
Command: config address_binding ip_mac ipaddress 10.1.1.1 mac_address 00-00-00-00-00-11 ports 1 mode acl

Success.

DGS-3700-12:5#
```

show address_binding

Purpose	To show address binding entries, blocked MAC entries, and port status.
Syntax	**show address_binding {[ip_mac [all | ipaddress <ipaddr> mac_address <macaddr>]|blocked [all | vlan_name <vlan_name> mac_address <macaddr>]|ports]}**
Description	This command will display IP-MAC Binding entries. Three different kinds of information can be viewed. • *ip_mac* – Address Binding entries can be viewed by entering the physical and IP addresses of the device. • *blocked* – Blocked address binding entries (bindings between VLAN names and MAC addresses) can be viewed by entering the VLAN name and the physical address of the device. • *ports* – The number of enabled ports on a device.
Parameters	*ip_mac* – The database that user create for address binding. *blocked* – The address database that system auto learned and blocked. *<ipaddr>* – The IP address of the device where the IP-MAC binding is made. *<macaddr>* – The MAC address of the device where the IP-MAC binding is made. *<vlan_name>* – The VLAN name of the VLAN that is bound to a MAC address in order to block a specific device on a known VLAN.
Restrictions	None.

Example usage:

To show the address binding global configuration:

```
DGS-3700-12:5#show address_binding
Command: show address_binding

ACL_Mode   : Enabled
Trap/Log   : Enabled
DHCP Snoop : Disabled

DGS-3700-12:5#
```

To show address binding entries:

The status will only be displayed when the system is in ACL mode. In ARP mode, all of the binding entries are effective. If the system is in ACL mode, those ACL mode binding entries will be effective, but the ARP mode binding entries will be inactive.

```
DGS-3700-12:5#show address_binding ip_mac all
Command: show address_binding ip_mac all

IP Address        MAC Address          Mode      Status     Ports
--------------  -----------------    --------   --------   ----------
10.1.1.1          00-00-00-00-00-11     ARP       Inactive  1,3,5,7,8
10.1.1.2          00-00-00-00-00-12     ACL       Active    1
10.1.1.10         00-00-00-00-00-aa     AUTO      Active    1

Total Entries : 3

DGS-3700-12:5#
```

To show blocked address binding:

```
DGS-3700-12:5#show address_binding blocked all
Command: show address_binding blocked all

VID    VLAN Name         MAC Address         Port
----   ---------         -----------------   ----------
 1      default          00-01-02-03-29-38       7
 1      default          00-0C-6E-5C-67-F4       7
 1      default          00-0C-F8-20-90-01       7
 1      default          00-0E-35-C7-FA-3F       7
 1      default          00-0E-A6-8F-72-EA       7
 1      default          00-0E-A6-C3-34-BE       7
 1      default          00-11-2F-6D-F3-AC       7
 1      default          00-50-8D-36-89-48       7
 1      default          00-50-BA-00-05-9E       7
 1      default          00-50-BA-10-D8-F6       7
 1      default          00-50-BA-38-7D-E0       7
 1      default          00-50-BA-51-31-62       7
 1      default          00-50-BA-DA-01-58       7
 1      default          00-A0-C9-01-01-23       7
 1      default          00-E0-18-D4-63-1C       7

Total Entries : 15


DGS-3700-12:5#
```

To display address binding ports:

```
DGS-3700-12:5#show address_binding ports
Command: show address_binding ports

Enabled Ports (Loose Mode)             : 4-8
Enabled Ports (Strict Mode)            : 1-3
Allow Zero IP Ports                    : 1-8
Forward DHCP Packet Ports              : 3-6


DGS-3700-12:5#
```

enable address_binding acl_mode

Purpose	Used to enable the ACL mode for an IP-MAC binding entry.
Syntax	**enable address_binding acl_mode**
Description	This command is used to enter address binding ACL mode. If user enables acl mode, the switch will first check if there are existing two empty access profiles. If the switch does not have two empty access profiles, it will show error message and can not enable acl mode; Otherwise the switch will create two access profiles automatically. After enable acl mode, the switch will check that there are any port is address_binding enabled. If this port is address_binding enabled, the switch will create access entry automatically (To block all ip packets on this port). If the acl pool is full and the switch can not create access entries, the switch will return warning message. If user already created some address_binding entries, then enable address_binding acl_mode, the switch will automatically create access entries (Each one entry which is mode is belong to acl in address_binding entries). If the acl pool is full before we created all address_binding entries, then address_binding module can not create access entries. The switch will show error message. And the switch will setup these address_binding entries as inactive.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable address binding ACL mode on the Switch:

```
DGS-3700-12:5# enable address_binding acl_mode
Command: enable address_binding acl_mode

Success.

DGS-3700-12:5#
```

disable address_binding acl_mode

Purpose	Used to disable the ACL mode for an IP-MAC binding entry.
Syntax	**disable address_binding acl_mode**
Description	This command is used to enter address binding normal mode. It user disable address binding ACL mode, the switch will delete the access profiles and access entries which were created by address binding module.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable address binding ACL mode on the Switch:

```
DGS-3700-12:5#disable address_binding acl_mode
Command: disable address_binding acl_mode

Success.

DGS-3700-12:5#
```

enable address_binding dhcp_snoop

Purpose	To enable address binding auto mode.
Syntax	**enable address_binding dhcp_snoop**
Description	By default, DHCP snooping is disabled. If user enables auto mode, all address_binding disabled ports will take as server ports (the switch will learned IP address through server ports (by DHCP OFFER and DHCP ACK packets)). Note that the DHCP discover packet can not be passed thru the user ports if the allow_zeroip function is disabled on this port. The auto-learned IP-MAC binding entry will be mapped to a specific source port based on the MAC address learning function. This entry will be created as an Auto-mode binding entry for this specific port. Each entry is associated with a lease time. When the lease time expired, the expired entry will be removed from this port. The auto-learned binding entry can be moved from one port to another port if the DHCP snooping function has learned that the MAC address is moved to a different port. Consider the case that a binding entry learned by DHCP snooping is conflict with the statically configured entry. The conflict case means that the binding relation is conflict. For example, if IP A is binded with MAC X by static configuration, supposed that the binding entry learned by DHCP snooping is IP A binded by MAC Y, then it is conflict. When the DHCP snooping learned entry is binded with the static configured entry, then the DHCP snooping learned entry will not be created. Consider the other conflict case when the DHCP snooping learned a binding entry, and the same IP-MAC binding pair has been statically configured. Supposed that the learned information is consitent with the static configured entry, then the auto-learned will not be created. Supposed that the entry is statically configured in ARP mode, then the auto learned entry will not be created. Supposed that the entry is statically configured on one port and the entry is auto-learned on another port, then the auto-learned entry will not be created either.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable address_binding auto_mode on the Switch:

```
DGS-3700-12:5#enable address_binding dhcp_snoop
Command: enable address_binding dhcp_snoop

Success.

DGS-3700-12:5#
```

disable address_binding dhcp_snoop

Purpose	To disable the address binding auto mode.
Syntax	**disable address_binding dhcp_snoop**
Description	When the DHCP snoop function is disabled, all of the auto-learned binding entries will be removed.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the address binding auto mode:

```
DGS-3700-12:5#disable address_binding dhcp_snoop
Command: disable address_binding dhcp_snoop

Success.

DGS-3700-12:5#
```

clear address_binding dhcp_snoop binding_entry ports

Purpose	To clear the address binding entries learned for the specified ports.
Syntax	**clear address_binding dhcp_snoop binding_entry ports [<portlist>|all]**
Description	This command is used to clear the address binding entries learned for the specified ports.
Parameters	*ports* – Specifies the list of ports that you would like to clear the DHCP-snoop learned entry.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear address binding DHCP snooping binding entries on ports 1-3:

```
DGS-3700-12:5#clear address_binding dhcp_snoop binding_entry ports 1-3
Command: clear address_binding dhcp_snoop binding_entry ports 1-3

Success.

DGS-3700-12:5#
```

show address_binding dhcp_snoop

Purpose	To show address binding auto learning database.
Syntax	**show address_binding dhcp_snoop {[max_entry { ports <portlist>} | binding_entry {port <port>}]}**
Description	This command is used to show all auto-learning database.
Parameters	*max_entry* – Displays the max number of entries which can be learned by dhcp snoop on the specified ports. *binding_entry* – Displays the address binding entries learned for the specified port.
Restrictions	None.

Example usage:

To show the address binding DHCP snoop state:

```
DGS-3700-12:5#show address_binding dhcp_snoop
Command: show address_binding dhcp_snoop

DHCP_Snoop : Enabled

DGS-3700-12:5#
```

To show address binding DHCP snoop by entry:

```
DGS-3700-12:5#show address_binding dhcp_snoop binding_entry
Command: show address_binding dhcp_snoop binding_entry

IP Address   MAC Address        Lease Time(secs)  Port     Status
-----------  -------------      ----------       --------  --------10.62.58.35  00-
0B-5D-05-34-0B   35964            1        Active
10.33.53.82  00-20-c3-56-b2-ef   2590             2        Inactive

Total entries : 2

DGS-3700-12:5#
```

To show address binding DHCP snoop max entry on specified ports:

```
DGS-3700-12:5#show address_binding dhcp_snoop max_entry ports 1-12
Command: show address_binding dhcp_snoop max_entry ports 1-12

Port  Max Entry
----  ---------
1     5
2     5
3     5
4     5
5     5
6     5
7     5
8     5
9     5
10    5
11    5
12    5

DGS-3700-12:5#
```

config address_binding dhcp_snoop max_entry

Purpose	Specifies the max number of entries which can be learned by the specified ports.
Syntax	**config address_binding dhcp_snoop max_entry ports [<portlist> | all] limit [<value 1-50> | no_limit]**
Description	This command specifies the max number of entries which can be learned by the specified ports. By default, per port max entry is 5.
Parameters	*<portlist>* – Specifies the list of ports that you would like to config for the max number of dhcp-snoop learned entries, which can be learned. *limit* – Specifies the max number.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To set the max number of entries that ports 1 to 3 can learn, up to 10:

```
DGS-3700-12:5#config address_binding dhcp_snoop max_entry ports 1-3 limit 10
Command: config address_binding dhcp_snoop max_entry ports 1-3 limit 10

Success.

DGS-3700-12:5#
```

enable address_binding trap_log

Purpose	Used to enable address_binding trap/log.
Syntax	**enable address_binding trap_log**
Description	This command is used to send trap and log when address binding module detects illegal ip and mac address.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable address binding trap/log:

```
DGS-3700-12:5#enable address_binding trap_log
Command: enable address_binding trap_log

Success.

DGS-3700-12:5#
```

disable address_binding trap_log

Purpose	Used to disable address binding trap/log.
Syntax	**disable address_binding trap_log**
Description	This command is used to disable address binding trap/log.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable address binding trap/log:

```
DGS-3700-12:5#disable address_binding trap_log
Command: disable address_binding trap_log

Success.

DGS-3700-12:5#
```

48

PORT SECURITY COMMANDS

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

Command	Parameters
config port_security ports	[<portlist>| all] [{admin_state [enable | disable] | max_learning_addr < max_lock_no 0-16384> | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) |{vlan [<vlan_name> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-16384> | no_limit]}(1)
delete port_security_entry	[vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>
clear port_security_entry	{ports [<portlist> | all] { [vlan <vlan_name> | vlanid <vidlist>]}}
show port_security	{ports [<portlist> | all] {[vlan <vlan_name> | vlanid <vidlist>] }}
show port_security_entry	{ports [<portlist> | all] {vlan <vlan_name> | vlanid <vidlist>]}}
enable port_security trap_log	
disable port_security trap_log	
config port_security system	max_learning_addr [<max_lock_no 1-16384> | no_limit]
config port_security vlan	[<vlan_name> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-16384> | no_limit]

Each command is listed, in detail, in the following sections.

config port_security ports

Purpose	Used to configure port security settings.
Syntax	**config port_security ports [<portlist>| all] [{admin_state [enable | disable] | max_learning_addr <max_lock_no 0-16384> | lock_address_mode [permanent | deleteontimeout | deleteonreset]}(1) |{vlan [<vlan_name> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-16384> | no_limit]}(1)**
Description	This command allows for the configuration of the port security feature. Only the ports listed in the *<portlist>* are affected.
Parameters	*portlist* – Specifies a port or range of ports to be configured. *all* – Configure port security for all ports on the Switch. *admin_state [enable | disable]* – Enable or disable port security for the listed ports. *max_learning_addr <max_lock_no 0-16384>* – Use this to limit the number of MAC addresses dynamically listed in the FDB for the ports. *lock_address_mode [Permanent | DeleteOnTimout | DeleteOnReset]* – Indicates the method of locking addresses. The user has three choices: *permanent* – The locked addresses will not age out after the aging timer expires. *DeleteOnTimeout* – The locked addresses will age out after the aging timer expires. *DeleteOnReset* – The locked addresses will not age out until the Switch has been restarted.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port security:

```
DGS-3700-12:5#config port_security ports 1-5 admin_state enable max_learning_addr 5
lock_address_mode deleteonreset
Command: config port_security ports 1-5 admin_state enable max_learning_addr 5
lock_address_mode deleteonreset

Success.

DGS-3700-12:5#
```

delete port_security_entry

Purpose	Used to delete a port security entry by MAC address and VLAN ID.
Syntax	**delete port_security_entry [vlan <vlan_name 32> | vlanid <vlanid 1-4094>] mac_address <macaddr>**
Description	This command is used to delete a single, previously learned port security entry, VLAN name, and MAC address.
Parameters	*vlan name <vlan_name 32>* – Enter the corresponding VLAN name of the port to delete. *vlanid <vlanid 1-4094>* – Enter the corresponding VID of the port to delete. *mac_address <macaddr>* – Enter the corresponding MAC address, previously learned by the port, to delete.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a port security entry:

```
DGS-3700-12:5#delete port_security_entry vlan rg mac_address 00-01-30-10-2C-C7
Command: delete port_security_entry vlan rg mac_address 00-01-30-10-2C-C7

Success.

DGS-3700-12:5#
```

clear port_security_entry

Purpose	Used to clear MAC address entries learned from a specified port for the port security function.
Syntax	**clear port_security_entry {ports [<portlist> | all] { [vlan <vlan_name> | vlanid <vidlist>]}}**
Description	This command is used to clear MAC address entries which were learned by the Switch by a specified port. This command only relates to the port security function.
Parameters	*<portlist>* – Specifies a port or port range to clear. *vlan* – The port security entry learned on the specified VLAN will be cleared. *vlanid* – Specifies a list of VLANs by their VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear a port security entry by port:

```
DGS-3700-12:5#clear port_security_entry port 6
Command: clear port_security_entry port 6

Success.

DGS-3700-12:5#
```

show port_security

Purpose	Used to display the current port security configuration.
Syntax	**show port_security_entry {ports [<portlist> | all] { [vlan <vlan_name> | vlanid <vidlist>] }}**
Description	This command is used to display port security information of the Switch's ports. The information displayed includes port security, admin state, maximum number of learning address and lock mode.
Parameters	*<portlist>* – Specifies a port or range of ports to be viewed. *vlan* – The port security entries learned on the specified VLANs will be cleared. *vlanid* – Specifies a list of VLANs by their VLAN ID.
Restrictions	None.

Example usage:

To display the port security configuration:

```
DGS-3700-12:5#show port_security ports 1-5
Command: show port_security ports 1-5

Port Configuration:
 Port   State     Lock Address Mode  Max. Learning Addr.
 -----  --------  -----------------  -------------------
 1      Disabled  DeleteOnReset      1
 2      Disabled  DeleteOnReset      1
 3      Disabled  DeleteOnReset      1
 4      Disabled  DeleteOnReset      1
 5      Disabled  DeleteOnReset      1

DGS-3700-12:5#
```

enable port_security trap_log

Purpose	Used to enable the trap/log for port security.
Syntax	**enable port_security trap_log**
Description	This command is used to enable port security traps/logs. When this command is enabled, if there's a new MAC that violates the pre-defined port security configuration, a trap will be sent out with the MAC and port informationt and the relevant information will be logged.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the port security trap/log setting:

```
DGS-3700-12:5#enable port_security trap_log
Command: enable port_security trap_log

Success.

DGS-3700-12:5#
```

disable port_security trap_log

Purpose	Used to disable the trap/log for port security.
Syntax	**disable port_security trap_log**
Description	This command is used to disable a port security trap/log. If the port security trap is disabled, no trap will be sent out for MAC violations.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the port security trap/log setting:

```
DGS-3700-12:5#disable port_security trap_log
Command: disable port_security trap_log

Success.

DGS-3700-12:5#
```

config port_security system max_learning_addr

Purpose	This command is used to set the maximum number of port security entries that can be learned by the system.
Syntax	**config port_security system max_learning_addr [<max_lock_no 1-16384> | no_limit (99999)]**
Description	This command sets the maximum number of port security entries that can be authorized system wide. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for specific VLANs on a port. If any limitation is exceeded, the new entry will be discarded. The setting for system level max learned users must be greater than the total of the max learned users allowed on all ports.
Parameters	*max_lock_no* – Specifies the maximum number of port security entries that can be learned by the system. If the setting is smaller than the number of current learned entries on all enabled ports, the command will be rejected. By default, the number is set to no_limit.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure port security:

```
DGS-3700-12:5#config port_security system max_learning_addr 2048
Command: config port_security system max_learning_addr 2048

Success.

DGS-3700-12:5#
```

show port_security entry

Purpose	This command is used to show the maximum port-security entries that can be learned by a specific VLAN on a specific port.
Syntax	**show port_security_entry {ports [ports [<portlist> | all] {[vlan <vlan_name> | vlanid <vidlist>]}}**
Description	This command is used to show port security entries on the Switch.
Parameters	*portlist* – Specifies a port or range of ports to be shown. *all* – Shows port security for all ports on the Switch. <*vlan_name*> – Specifies a list of VLANs by VLAN name to show the port security entry. *vlanid* – Specifies a list of VLANs by VLAN ID to show the port security entry.
Restrictions	None.

Example usage:

To display port security entries on the Switch:

```
DGS-3700-12:5#show port_security_entry
Command: show port_security_entry

 No entry is found!


DGS-3700-12:5#
```

config port_security vlan

Purpose	This command is used to set the maximum port-security entries that can be learned on a specific VLAN.
Syntax	**config port_security vlan [<vlan_name> | vlanid <vidlist>] max_learning_addr [<max_lock_no 0-16384>| no_limit]**
Description	This command sets the maximum port-security entries that can be learned on a specific VLAN. There are four levels of limitations on the learned entry number, for the entire system, for a port, for a VLAN, and for a specific VLAN on a port. If any limitation is exceeded, the new entry will be discarded.
Parameters	<*vlan_name*> – Specifies a list of VLANs by VLAN ID to limit the address learning. *vlanid* – Specifies a list of VLAN by VLAN ID. *max_learning_addr* – Specifies the maximum number of port-security entries that can be learned with this VLAN. If this parameter is set to 0, it means that no user can get authorization on this VLAN. If the setting is smaller than the number of current learned entries on the VLAN, the command will be rejected. The default value is “no_limit”

config port_security vlan

	no_limit – No limitation on the number.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port security:

```
DGS-3700-12:5#config port_security vlan vlanid 1 max_learning_addr 64
Command: config port_security vlan vlanid 1 max_learning_addr 64

Success.

DGS-3700-12:5#
```

49

802.1X COMMANDS (INCLUDING GUEST VLANS)

The Switch implements the server-side of the IEEE 802.1X Port-based and MAC-based Network Access Control. This mechanism is intended to allow only authorized users, or other network devices, access to network resources by establishing criteria for each port on the Switch that a user or network device must meet before allowing that port to forward or receive frames.

Command	Parameters
enable 802.1x	
disable 802.1x	
create 802.1x user	<username 15>
delete 802.1x user	<username 15>
show 802.1x user	
config 802.1x max_users	[<value 1 -1536> |no_limit]
config 802.1x fwd_pdu system	[enable | disable]
config 802.1x fwd_pdu ports	[<portlist>|all] [enable | disable]
show 802.1x [auth_state | auth_configuration]	{ports [<portlist |all>]}
config 802.1x capability ports	[<portlist> | all] [authenticator | none]
config 802.1x auth_parameter ports	[<portlist>|all] [default|{direction [both|in]|port_control [force_unauth|auto|force_auth]|quiet_period <sec 0-65535>|tx_period <sec 1-65535>|supp_timeout <sec 1-65535>|server_timeout <sec 1-65535>|max_req <value 1-10>|reauth_period <sec 1-65535>|max_users [<value 1-128> |no_limit]|enable_reauth [enable|disable]}(1)]
config 802.1x auth_protocol	[local | radius_eap]
config 802.1x init	[port_based ports [<portlist> | all] | mac_based [ports] [<portlist> |all] {mac_address <macaddr>}]
config 802.1x auth_mode	[port_based | mac_based]
config 802.1x reauth	[port_based ports [<portlist> | all] | mac_based [ports] [<portlist> | all] {mac_address <macaddr>}]
config radius add	<server_index 1-3> [<server_ip> | <ipv6addr>] key <passwd 32> [default | { auth_port<udp_port_number 1-65535> | acct_port <udp_port_number 1-65535> | timeout<int 1-255> | retransmit<int 1-255>}](1)
config radius delete	<server_index 1-3>
config radius	<server_index 1-3> {ipaddress [<server_ip>|<ipv6addr>] |key <passwd 32> | auth_port <udp_port_number 1-65535 > | acct_port <udp_port_number 1-65535 >|timeout <int 1-255> |retransmit <int 1-255>}(1)
show radius	
create 802.1x guest_vlan	<vlan_name 32>
config 802.1x guest_vlan ports	[<portlist> | all] state [enable | disable]

Command	Parameters
delete 802.1x guest_vlan	<vlan_name 32>
show 802.1x guest_vlan	
show auth_statistics	{ports [<portlist>|all]}
show auth_diagnostics	{ports [<portlist>|all]}
show auth_session_statistics	{ports [<portlist>|all]}
show auth_client	
show acct_client	
config accounting service	[network | shell | system] state [enable|disable]
show accounting service	

Each command is listed, in detail, in the following sections:

enable 802.1x

Purpose	Used to enable the 802.1X server on the Switch.
Syntax	**enable 802.1x**
Description	This command is used to enable the 802.1X Network Access control server application on the Switch. To select between port-based or MAC-based, use the **config 802.1x auth_mode** command.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable 802.1X switch wide:

```
DGS-3700-12:5#enable 802.1x
Command: enable 802.1x

Success.

DGS-3700-12:5#
```

disable 802.1x

Purpose	Used to disable the 802.1X server on the Switch.
Syntax	**disable 802.1x**
Description	This command is used to disable the 802.1X Network Access control server application on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable 802.1X on the Switch:

```
DGS-3700-12:5#disable 802.1x
Command: disable 802.1x

Success.

DGS-3700-12:5#
```

create 802.1x user

Purpose	Used to create 802.1X user.
Syntax	**create 802.1x user <username 15>**
Description	This command is used to create a 802.1X user.
Parameters	*username* – Specifies adding user name
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create user “test”:

```
DGS-3700-12:5#create 802.1x user test
Command: create 802.1x user test

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

Success.

DGS-3700-12:5#
```

delete 802.1x user

Purpose	Used to delete 802.1X user.
Syntax	**delete 802.1x user <username 15>**
Description	This command is used to delete specified user.
Parameters	*username* – Specifies deleting user name
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete user “test”:

```
DGS-3700-12:5#delete 802.1x user test
Command: delete 802.1x user test

Success.

DGS-3700-12:5#
```

show 802.1x user

Purpose	Used to show 802.1X user.
Syntax	**show 802.1x user**
Description	This command is used to display the 802.1X user account information.
Parameters	None.
Restrictions	None.

Example usage:

To display the 802.1X user information:

```
DGS-3700-12:5#show 802.1x user
Command: show 802.1x user


 Current Accounts:
 Username         Password
 -------------  --------------
 test              123

 Total Entries:1

DGS-3700-12:5#
```

config 802.1x max_users

Purpose	Used to configure the max number of users that can be learned via 802.1X authentication.
Syntax	**config 802.1x max_users [<value 1 -1536> |no_limit]**
Description	This command is used to configure a global limitation on the maximum number of users that can be learned via 802.1X authentication. In addition to the global limitation, per port max users is also limited. It is specified by config 802.1X auth_parameter command.
Parameters	*max_users* – Specifies the maximum number of users. The range is 1 to 1536. By default, there is no limit on the max users.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config the 802.1X max users:

```
DGS-3700-12:5#config 802.1x max_users 100
Command: config 802.1x max_users 100

Success.

DGS-3700-12:5#
```

config 802.1x auth_protocol

Purpose	Used to cofig the 802.1X auth protocol
Syntax	**config 802.1x auth_protocol [local|radius_eap]**
Description	This command is used to configure the 802.1X auth protocol.
Parameters	*local* – Specifies the auth protocol as local. *radius_eap* – Specifies the auth protocol as RADIUS EAP.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To config the 802.1X RADIUS EAP:

```
DGS-3700-12:5#config 802.1x auth_protocol radius_eap
Command: config 802.1x auth_protocol radius_eap

Success.
DGS-3700-12:5#
```

config 802.1x fwd_pdu system

Purpose	Used to configure forwarding of EAPOL PDU when 802.1X is disabled.
Syntax	**config 802.1x fwd_pdu system [enable | disable]**
Description	This command is a global setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X fwd_pdu is enabled and 802.1X is disabled (globally or just for the port). The default state is disable.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure forwarding of EAPOL PDU

```
DGS-3700-12:5#config 802.1x fwd_pdu system enable
Command: config 802.1x fwd_pdu system enable

Success.

DGS-3700-12:5#
```

config 802.1x fwd_pdu ports

Purpose	Used to configure if the port will flood EAPOL PDU when 802.1X functionality is disabled.
Syntax	**config 802.1x fwd_pdu ports [<portlilst>| all] [enable | disable]**
Description	This command is a per port setting to control the forwarding of EAPOL PDU. When 802.1X functionality is disabled globally or for a port, and if 802.1X fwd_pdu is enabled both globally and for the port, a received EAPOL packet on the port will be flooded in the same VLAN to those ports for which 802.1X fwd_pdu is enabled and 802.1X is disabled (globally or just for the port). The default state is disable.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X fwd PDU for ports:

```
DGS-3700-12:5#config 802.1x fwd_pdu ports 1-2 enable
Command: config 802.1x fwd_pdu  ports 1-2 enable

Success.

DGS-3700-12:5#
```

show 802.1x

Purpose	Used to display the 802.1X state or configurations.
Syntax	**show 802.1x [auth_state | auth_configuration] {ports <portlist|all>}**
Description	This command is used to display the 802.1X state or configurations.
Parameters	*auth_state* – Used to display 802.1X authentication state machine of some or all ports *auth_configuration* – Used to display 802.1X configurations of some or all ports. *portlist* – Specifies a range of ports to be displayed. *all* – Specifies all of ports to be displayed
Restrictions	None.

Example usage:

To display the 802.1X states:

```
DGS-3700-12:5#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-3700-12:5#
```

To display the 802.1X configurations:

```
DGS-3700-12:5#show 802.1x auth_configuration ports 1
Command: show 802.1x auth_configuration ports 1

802.1X                  : Enabled
Authentication Mode     : Port_based
Authentication Protocol : Radius_EAP
Forward EAPOL PDU       : Disabled
Max Users     : 1536

Port Number    : 1
Capability     : None
AdminCrlDir    : Both
OpenCrlDir     : Both
Port Control   : Auto
QuietPeriod    : 60    sec
TxPeriod       : 30    sec
SuppTimeout    : 30    sec
ServerTimeout  : 30    sec
MaxReq         : 2     times
ReAuthPeriod   : 3600  sec
ReAuthenticate : Disabled
Forward EAPOL PDU On Port : Disabled
Max Users On port : 128

DGS-3700-12:5#
```

config 802.1x capability

Purpose	Used to configure the port capability.
Syntax	**config 802.1x capability ports [<portlist>|all] [authenticator|none]**
Description	This command is used to configure the port capability.
Parameters	*portlist* – Specifies a range of ports to be displayed. *all* – Specifies all of ports to be displayed *authenticator* – The port that wishes to enforce authentication before allowing cess to services that are accessible via that Port adops the authenticator role. *none* – Allows the flow of PDUs via the Port
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port capabilty:

```
DGS-3700-12:5#config 802.1x capability ports 1-10 authenticator
Command: config 802.1x capability ports 1-10 authenticator

Success.

DGS-3700-12:5#
```

config 802.1x auth_parameter

Purpose	Used to configure the parameters that control the operation of the authenticator associated with a port.
Syntax	**config 802.1x auth_parameter [<portlist>|all] [default|{direction [both|in]|port_control[force_unauth|auto|force_auth]|quiet_period <sec 0-65535>|tx_period <sec 1-65535>|supp_timeout <sec 1-65535>|server_timeout <sec 1-65535>|max_req <value 1-10>|reauth_period <sec 1-65535>|max_users [<value 1-128>|no_limit]|enable_reauth [enable|disable]}(1)]**
Description	This command is used to configure the parameters that control the operation of the authenticator associated with a port.
Parameters	*portlist* – Specifies a range of ports to be displayed. *all* – Specifies all of ports to be displayed. *default* – Sets all parameter to be default value. *direction* – Sets the direction of access control . **both:** For bidirectional access control. **in:** For unidirectional access control. *port_control* – You can force a specific port to be unconditionally authorized or unauthorized by setting the the parameter of port_control to be force_authorized or force_unauthorized. Besides, the controlled port will reflect the outcome of authentication if port_control is auto. *quiet_period* – It is the initialization value of the quietWhile timer. The default value is *60* s and can be any value from *0* to *65535*. *tx_period* – It is the initialization value of the txWhen timer. The default value is *30* s and can be any value among *1* to *65535*. *supp_timeout* – The initialization value of the aWhile timer when timing out the supplicant. Its default value is *30* s and can be any value among *1* to *65535*. *server_timeout* – The initialization value of the aWhile timer when timing out the authentication server. Its default value is *30* and can be any value among *1* to *65535*. *max_req* – The maximum number of times that the authenitcation PAE state machine will retransmit an EAP Request packet to the supplicant. Its default value is *2* and can be any number among *1* to *10*. *max_users <value 1-128>* – Specifies the maximum number of users. The range is 1 to 128 or no_limit. The default is 128 users. *reauth_period* – Its a nonzero number of seconds, which is used to be the re-authentication timer. The default value is 3600. *enable_reauth* – You can enable or disable the re-authentication mechanism for a specific port.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the parameters that control the operation of the authenticator associated with a port::

```
DGS-3700-12:5#config 802.1x auth_parameter ports 1-2 direction both
Command: config 802.1x auth_parameter ports 1-2 direction both

Success.

DGS-3700-12:5#
```

config 802.1x auth_mode

Purpose	Used to configure 802.1X authentication mode.
Syntax	**config 802.1x auth_mode [port_based | mac_based]**
Description	This command is used to configure the authentication mode.
Parameters	*port_based* – Configure the authentication as port based mode. *mac_based* – Configure the authentication as MAC based mode.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the authentication mode:

```
DGS-3700-12:5#config 802.1x auth_mode port_based
Command: config 802.1x auth_mode port_based

Success.

DGS-3700-12:5#
```

config 802.1x init

Purpose	Used to initialize the authentication state machine of some or all ports.
Syntax	**config 802.1x init [port_based ports [<portlist>|all] |mac_based [ports] [<portlist>|all] {mac_address <macaddr>}]**
Description	This command is used to initialize the authentication state machine of some or all.
Parameters	*port_based* – This instructs the Switch to init 802.1X functions based only on the port number. Ports approved for init can then be specified *mac_based* – This instructs the Switch to init 802.1X functions based only on the MAC address. MAC addresses approved for init can then be specified. *portlist* – Specifies a range of ports to be displayed. *all* – Specifies all of ports to be displayed. *mac_address* – MAC address of client
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To initialize the authentication state machine of some or all:

```
DGS-3700-12:5#config 802.1x init port_based ports all
Command: config 802.1x init port_based ports all

Success.

DGS-3700-12:5#
```

config 802.1x reauth

Purpose	Used to configure the 802.1X re-authentication feature of the Switch.
Syntax	**config 802.1x reauth [port_based ports [<portlist> | all] | mac_based [ports] [<portlist> | all] {mac_address <macaddr>}]**
Description	This command is used to re-authenticate a previously authenticated device based on port number.
Parameters	*port_based* – This instructs the Switch to re-authorize 802.1X functions based only on the port number. Ports approved for re-authorization can then be specified. *mac_based* – This instructs the Switch to re-authorize 802.1X functions based only on the MAC address. MAC addresses approved for re-authorization can then be specified. *ports <portlist>* – Specifies a port or range of ports to be re-authorized. *all* – Specifies all of the ports on the Switch. *mac_address <macaddr>* – Enter the MAC address to be re-authorized.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure 802.1X reauthentication for ports 1 to 8:

```
DGS-3700-12:5#config 802.1x reauth port_based ports 1-8
Command: config 802.1x reauth port_based ports 1-8

Success.

DGS-3700-12:5#
```

create 802.1x guest_vlan

Purpose	Used to configure a pre-existing VLAN as a 802.1X Guest VLAN.
Syntax	**create 802.1x guest_vlan <vlan_name 32>**
Description	This command is used to configure a pre-defined VLAN as a 802.1X Guest VLAN. 802.1X Guest VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like limited access rights on the Switch.
Parameters	*<vlan_name 32>* – Enter an alphanumeric string of no more than 32 characters to define a pre-existing VLAN as a 802.1X Guest VLAN. This VLAN must have first been created with the **create vlan** command mentioned earlier in this manual.
Restrictions	Only Administrator and Operator-level users can issue this command. This VLAN is only supported for port-based 802.1X and must have already been previously created using the **create vlan** command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To configure a previously created VLAN as a 802.1X Guest VLAN for the Switch.

```
DGS-3700-12:5#create 802.1x guest_vlan Trinity
Command: create 802.1x guest_vlan Trinity

Success.

DGS-3700-12:5#
```

config 802.1x guest_vlan ports

Purpose	Used to configure ports for a pre-existing 802.1X guest VLAN.
Syntax	**config 802.1x guest_vlan ports [<portlist> | all] state [enable | disable]**
Description	This command is used to configure ports to be enabled or disabled for the 802.1X guest VLAN.
Parameters	*<portlist>* – Specify a port or range of ports to be configured for the 802.1X Guest VLAN. *all* – Specify this parameter to configure all ports for the 802.1X Guest VLAN. *state [enable | disable]* – Use these parameters to enable or disable port listed here as enabled or disabled for the 802.1X Guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command. This VLAN is only supported for port-based 802.1X and must have already been previously created using the **create vlan** command. If the specific port state changes from an enabled state to a disabled state, these ports will return to the original VLAN.

Example usage:

To configure the ports for a previously created 802.1X Guest VLAN as enabled.

```
DGS-3700-12:5#config 802.1x guest_vlan ports 1-5 state enable
Command: config 802.1x guest_vlan ports 1-5 state enable

Success.

DGS-3700-12:5#
```

show 802.1x guest_vlan

Purpose	Used to view the configurations for a 802.1X Guest VLAN.
Syntax	**show 802.1x guest_vlan**
Description	This command is used to display the settings for the VLAN that has been enabled as an 802.1X Guest VLAN. 802.1X Guest VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like limited access rights on the Switch.
Parameters	None.
Restrictions	This VLAN is only supported for port-based 802.1X and must have already been previously created using the **create vlan** command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To show 802.1X Guest VLAN.

```
DGS-3700-12:5#show 802.1x guest_vlan
Command: show 802.1x guest_vlan

Guest VLAN Setting
-----------------------------------------------------------
Guest VLAN : Trinity
Enable guest VLAN ports: 5-8

Success.

DGS-3700-12:5#
```

delete 802.1x guest_vlan

Purpose	Used to delete a 802.1X Guest VLAN.
Syntax	**delete 802.1x guest_vlan <vlan_name 32>**
Description	This command is used to delete an 802.1X Guest VLAN. 802.1X Guest VLAN clients are those who have not been authorized for 802.1X or they haven't yet installed the necessary 802.1X software, yet would still like limited access rights on the Switch.
Parameters	*<vlan_name 32>* – Enter the VLAN name of the 802.1X Guest VLAN to be deleted.
Restrictions	Only Administrator and Operator-level users can issue this command. This VLAN is only supported for port-based 802.1X and must have already been previously created using the **create vlan** command. Only one VLAN can be set as the 802.1X Guest VLAN.

Example usage:

To delete a previously created 802.1X Guest VLAN.

```
DGS-3700-12:5#delete 802.1x guest_vlan Trinity
Command: delete 802.1x guest_vlan Trinity

Success.

DGS-3700-12:5#
```

config radius add

Purpose	Used to configure the settings the Switch will use to communicate with a RADIUS server.
Syntax	**config radius add <server_index 1-3> [<server_ip>|<ipv6addr>] key <passwd 32> [default | { auth_port <udp_port_number 1-65535 > | acct_port <udp_port_number 1-65535 >| timeout <int 1-255> | retransmit <int 1-255>}](1)**
Description	This command is used to configure the settings the Switch will use to communicate with a RADIUS server.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch. *<server_ip>* – The IP address of the RADIUS server. *<ipv6addr>* – The IPv6 address of the RADIUS server. *key* – Specifies that a password and encryption key will 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 32 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*. *timeout* <int 1-255> – The time in second for waiting for a server reply. Default value is *5* seconds. *retransmit* <int 1-255> – The count for re-transmit. Default value is *2*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS server communication settings:

```
DGS-3700-12:5#config radius add 1 10.48.74.121 key dlink default
Command: config radius add 1 10.48.74.121 key dlink default

Success.

DGS-3700-12:5#
```

config radius delete

Purpose	Used to delete a previously entered RADIUS server configuration.
Syntax	**config radius delete <server_index 1-3>**
Description	This command is used to delete a previously entered RADIUS server configuration.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to 3 groups of RADIUS server settings can be entered on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete previously configured RADIUS server communication settings:

```
DGS-3700-12:5#config radius delete 1
Command: config radius delete 1

Success.

DGS-3700-12:5#
```

config radius

Purpose	Used to configure the Switch's RADIUS settings.
Syntax	**config radius <server_index 1-3> {ipaddress[<server_ip>|<ipv6addr>] |key <passwd 32> | auth_port <udp_port_number 1-65535 > | acct_port <udp_port_number 1-65535 >| timeout <int 1-255> |retransmit <int 1-255>}(1)**
Description	This command is used to configure the Switch's RADIUS settings.
Parameters	*<server_index 1-3>* – Assigns a number to the current set of RADIUS server settings. Up to three groups of RADIUS server settings can be entered on the Switch. *ipaddress <server_ip>* – The IP address of the RADIUS server. • *<ipv6addr>* – The IPv6 address of the RADIUS server. *key* – Specifies that a password and encryption key will 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 32 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*. *timeout* <int 1-255> – The time in second for waiting for a server reply. Default value is *5* seconds. *retransmit* <int 1-255> – The count for re-transmit. Default value is *2*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the RADIUS settings:

```
DGS-3700-12:5#config radius 1 ipaddress 10.48.74.121 key dlink_default
Command: config radius 1 ipaddress 10.48.74.121 key dlink_default

Success.

DGS-3700-12:5#
```

show radius

Purpose	Used to display the current RADIUS configurations on the Switch.
Syntax	**show radius**
Description	This command is used to display the current RADIUS configurations on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To display RADIUS settings on the Switch:

```
DGS-3700-12:5#show radius
Command: show radius

Index 1
    IP Address      : 10.48.74.121
    Auth-Port       : 1812
    Acct-Port       : 1813
    Timeout         : 5
    Retransmit      : 2
    Key             : dlink_default

DGS-3700-12:5#
```

show auth_statistics

Purpose	Used to display authenticator statistics information.
Syntax	**show auth_statistics {ports [<portlist>|all]}**
Description	This command is used to display authenticator statistics information.
Parameters	*portlist* – Specifies a range of ports to be configured. *all* – All ports.
Restrictions	None.

Example usage:

To display authenticator statistics information from port 1:

```
DGS-3700-12:5#show auth_statistics ports 1
Command: show auth_statistics ports 1

ort Number : 1

 EapolFramesRx                      0
 EapolFramesTx                      0
 EapolStartFramesRx                 0
 EapolReqIdFramesTx                 0
 EapolLogoffFramesRx                0
 EapolReqFramesTx                   0
 EapolRespIdFramesRx                0
 EapolRespFramesRx                  0
 InvalidEapolFramesRx               0
 EapLengthErrorFramesRx             0

 LastEapolFrameVersion              0
 LastEapolFrameSource               00-00-00-00-00-00

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

show auth_diagnostics

Purpose	Used to display authenticator diagnostics information
Syntax	**show auth_ diagnostics {ports [<portlist>|all]}**
Description	This command is used to display authenticator diagnostics information
Parameters	*portlist* – Specifies a range of ports to be configured. *all* – All ports.
Restrictions	None.

Example usage:

To display authenticator diagnostics information from port 1:

```
DGS-3700-12:5#show auth_diagnostics ports 1
Command: show auth_diagnostics ports 1

Port Number: 1

 EntersConnecting                      0
 EapLogoffsWhileConnecting             0
 EntersAuthenticating                  0
 SuccessWhileAuthenticating            0
 TimeoutsWhileAuthenticating           0
 FailWhileAuthenticating               0
 ReauthsWhileAuthenticating            0
 EapStartsWhileAuthenticating          0
 EapLogoffWhileAuthenticating          0
 ReauthsWhileAuthenticated             0
 EapStartsWhileAuthenticated           0
 EapLogoffWhileAuthenticated           0
 BackendResponses                      0
 BackendAccessChallenges               0
 BackendOtherRequestsToSupplicant      0
 BackendNonNakResponsesFromSupplicant  0
 BackendAuthSuccesses                  0
 BackendAuthFails                      0

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

show auth_session_statistics

Purpose	Used to display authenticator session statistics information
Syntax	**show auth_session_statistics {ports [<portlist>|all]}**
Description	This command is used to display authenticator session statistics information
Parameters	*portlist* – Specifies a range of ports to be configured. *all* – All port.
Restrictions	None.

Example usage:

To display authenticator session statistics information from port 1:

```
DGS-3700-12:5#show auth_session_statistics ports 1
Command: show auth_session_statistics ports 1

Port number : 1

SessionOctetsRx                 0
SessionOctetsTx                 0
SessionFramesRx                 0
SessionFramesTx                 0
SessionId
SessionAuthenticMethod     Remote Authentication Server
SessionTime                     0
SessionTerminateCause      SupplicantLogoff
SessionUserName

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

show auth_client

Purpose	Used to display authentication client information
Syntax	**show auth_client**
Description	This command is used to display authentication client information
Parameters	None.
Restrictions	None.

Example usage:

To display authentication client information:

```
DGS-3700-12:5#show auth_client
Command: show auth_client

radiusAuthClient ==>
radiusAuthClientInvalidServerAddresses   0
radiusAuthClientIdentifier


radiusAuthServerEntry ==>
radiusAuthServerIndex :1

radiusAuthServerAddress                  0.0.0.0
radiusAuthClientServerPortNumber         0
radiusAuthClientRoundTripTime            0
radiusAuthClientAccessRequests           0
radiusAuthClientAccessRetransmissions    0
radiusAuthClientAccessAccepts            0
radiusAuthClientAccessRejects            0
radiusAuthClientAccessChallenges         0
radiusAuthClientMalformedAccessResponses 0
radiusAuthClientBadAuthenticators        0
radiusAuthClientPendingRequests          0
radiusAuthClientTimeouts                 0
radiusAuthClientUnknownTypes             0
radiusAuthClientPacketsDropped           0

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

show acct_client

Purpose	Used to display account client information.
Syntax	**show acct_client**
Description	This command is used to display account client information
Parameters	None.
Restrictions	None.

Example usage:

To display account client information:

```
DGS-3700-12:5#show acct_client
Command: show acct_client

radiusAcctClient ==>
radiusAcctClientInvalidServerAddresses   0
radiusAcctClientIdentifier

radiusAuthServerEntry ==>
radiusAccServerIndex : 1

radiusAccServerAddress                0.0.0.0
radiusAccClientServerPortNumber       0
radiusAccClientRoundTripTime           0
radiusAccClientRequests                0
radiusAccClientRetransmissions         0
radiusAccClientResponses               0
radiusAccClientMalformedResponses      0
radiusAccClientBadAuthenticators       0
radiusAccClientPendingRequests         0
radiusAccClientTimeouts                0
radiusAccClientUnknownTypes            0
radiusAccClientPacketsDropped          0

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

config accounting service

Purpose	Used to configure the state of the specified RADIUS accounting service.
Syntax	**config accounting service [network | shell | system] (1) state [enable|disable]**
Description	This command is used to enable or disable the specified RADIUS accounting service.
Parameters	*network* – Accounting service for 802.1X port access control. By default, the service is disabled. *shell* – Accounting service for shell events: When user login or logout the switch (via the console, Telnet, or SSH) and when timeout occurs, accounting information will be collected and sent to RADIUS server. By default, the service is disabled. *system* – Accounting service for system events: reset, reboot. By default, the service is disabled. *enable* – Enable the specified accounting service. *disable* – Disable the specified accounting service.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the accounting service:

```
DGS-3700-12:5#config accounting service shell state enable
Command: config accounting service shell state enable

Success.

DGS-3700-12:5#
```

show accounting service

Purpose	Used to show the RADIUS accounting services' status.
Syntax	**show accounting service**
Description	This command is used to show the state for radius accounting service.
Parameters	None.
Restrictions	None.

Example usage:

To show accounting service:

```
DGS-3700-12:5#show accounting service
Command: show accounting service

Accounting Service
------------------
Network   : Enabled
Shell     : Enabled
System    : Enabled

DGS-3700-12:5#
```

50

SSL COMMANDS

Secure Sockets Layer or SSL is a security feature that will provide a secure communication path between a host and client through the use of authentication, digital signatures and encryption. These security functions are implemented through the use of a *ciphersuite*, which is a security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session and consists of three levels:

1. **Key Exchange:** The first part of the cyphersuite string specifies the public key algorithm to be used. This Switch utilizes the Rivest Shamir Adleman (RSA) public key algorithm and the Digital Signature Algorithm (DSA), specified here as the *DHE_DSS* Diffie-Hellman (DHE) public key algorithm. This is the first authentication process between client and host as they "exchange keys" in looking for a match and therefore authentication to be accepted to negotiate encryptions on the following level.
2. **Encryption:** The second part of the ciphersuite that includes the encryption used for encrypting the messages sent between client and host. The Switch supports two types of cryptology algorithms:
   - **Stream Ciphers** – There are two types of stream ciphers on the Switch, RC4 with 40-bit keys and RC4 with 128-bit keys. These keys are used to encrypt messages and need to be consistent between client and host for optimal use.
   - **CBC Block Ciphers** – CBC refers to Cipher Block Chaining, which means that a portion of the previously encrypted block of encrypted text is used in the encryption of the current block. The Switch supports the 3DES_EDE encryption code defined by the Data Encryption Standard (DES) to create the encrypted text.
3. **Hash Algorithm**: This part of the ciphersuite allows the user to choose a message digest function which will determine a Message Authentication Code. This Message Authentication Code will be encrypted with a sent message to provide integrity and prevent against replay attacks. The Switch supports two hash algorithms, *MD5* (Message Digest 5) and *SHA* (Secure Hash Algorithm).

These three parameters are uniquely assembled in four choices on the Switch to create a three layered encryption code for secure communication between the server and the host. The user may implement any one or combination of the ciphersuites available, yet different ciphersuites will affect the security level and the performance of the secured connection. The information included in the ciphersuites is not included with the Switch and requires downloading from a third source in a file form called a *certificate*. This function of the Switch cannot be executed without the presence and implementation of the certificate file and can be downloaded to the Switch by utilizing a TFTP server. The Switch supports SSLv3 and TLSv1. Other versions of SSL may not be compatible with this Switch and may cause problems upon authentication and transfer of messages from client to host.

Command	Parameters
enable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}(1)}
disable ssl	{ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}(1)}
config ssl cachetimeout	<value 60-86400>
show ssl	
show ssl certificate	
show ssl cachetimeout	
download ssl certificate	<ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>

Each command is listed, in detail, in the following sections.

enable ssl

Purpose	To enable the SSL function on the Switch.
Syntax	**enable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}(1)}**
Description	This command will enable SSL on the Switch by implementing any one or combination of listed ciphersuites on the Switch. Entering this command without a parameter will enable the SSL status on the Switch. Enabling SSL will disable the web-manager on the Switch.
Parameters	*ciphersuite* – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. *RSA_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. *DHE_DSS_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. *RSA_EXPORT_with_RC4_40_MD5* – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys. The ciphersuites are enabled by default on the Switch, yet the SSL status is disabled by default. Enabling SSL with a ciphersuite will not enable the SSL status on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable SSL on the Switch for all ciphersuites:

```
DGS-3700-12:5#enable ssl
Command: enable ssl

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

DGS-3700-12:5#
```

NOTE: Enabling SSL on the Switch will enable all ciphersuites. To utilize a particular ciphersuite, the user must eliminate other ciphersuites by using the **disable ssl** command along with the appropriate ciphersuites.

NOTE: Enabling the SSL function on the Switch will disable the port for the web manager (port 80). To log on to the web based manager, the entry of the URL must begin with *https://*. (ex. https://10.90.90.90)

disable ssl

Purpose	To disable the SSL function on the Switch.
Syntax	**disable ssl {ciphersuite {RSA_with_RC4_128_MD5 | RSA_with_3DES_EDE_CBC_SHA | DHE_DSS_with_3DES_EDE_CBC_SHA | RSA_EXPORT_with_RC4_40_MD5}(1)}**
Description	This command will disable SSL on the Switch and can be used to disable any one or combination of listed ciphersuites on the Switch.
Parameters	*ciphersuite* – A security string that determines the exact cryptographic parameters, specific encryption algorithms and key sizes to be used for an authentication session. The user may choose any combination of the following: *RSA_with_RC4_128_MD5* – This ciphersuite combines the RSA key exchange, stream cipher RC4 encryption with 128-bit keys and the MD5 Hash Algorithm. *RSA_with_3DES_EDE_CBC_SHA* –This ciphersuite combines the RSA key exchange, CBC Block Cipher 3DES_EDE encryption and the SHA Hash Algorithm. *DHE_DSS_with_3DES_EDE_CBC_SHA* – This ciphersuite combines the DSA Diffie Hellman key exchange, CBC Block Cipher 3DES_EDE encryption and SHA Hash Algorithm. *RSA_EXPORT_with_RC4_40_MD5* – This ciphersuite combines the RSA Export key exchange, stream cipher RC4 encryption with 40-bit keys.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the SSL status on the Switch:

```
DGS-3700-12:5#disable ssl
Command: disable ssl

Success.

DGS-3700-12:5#
```

To disable ciphersuite RSA_EXPORT_with_RC4_40_MD5 only:

```
DGS-3700-12:5#disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5
Command: disable ssl ciphersuite RSA_EXPORT_with_RC4_40_MD5

Success.

DGS-3700-12:5#
```

config ssl cachetimeout

Purpose	Used to configure the SSL cache timeout.
Syntax	**config ssl cachetimeout timeout <value 60-86400>**
Description	This command will set the time between a new key exchange between a client and a host using the SSL function. A new SSL session is established every time the client and host go through a key exchange. Specifying a longer timeout will allow the SSL session to reuse the master key on future connections with that particular host, therefore speeding up the negotiation process.
Parameters	*timeout <value 60-86400>* – Enter a timeout value between *60* and *86400* seconds to specify the total time an SSL key exchange ID stays valid before the SSL module will require a new, full SSL negotiation for connection. The default cache timeout is *600* seconds
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the SSL cachetimeout for 7200 seconds:

```
DGS-3700-12:5#config ssl cachetimeout 7200
Command: config ssl cachetimeout 7200

Success.

DGS-3700-12:5#
```

show ssl cachetimeout

Purpose	Used to show the SSL cache timeout.
Syntax	**show ssl cachetimeout**
Description	This command is used to view the SSL cache timeout currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL cache timeout on the Switch:

```
DGS-3700-12:5#show ssl cachetimeout
Command: show ssl cachetimeout

Cache timeout is 600 second(s).

DGS-3700-12:5#
```

show ssl

Purpose	Used to view the SSL status and the certificate file status on the Switch.
Syntax	**show ssl**
Description	This command is used to view the SSL status on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the SSL status on the Switch:

```
DGS-3700-12:5#show ssl
Command: show ssl

SSL status                     Enabled
RSA_WITH_RC4_128_MD5           Enabled
RSA_WITH_3DES_EDE_CBC_SHA      Enabled
DHE_DSS_WITH_3DES_EDE_CBC_SHA  Enabled
RSA_EXPORT_WITH_RC4_40_MD5     Enabled

DGS-3700-12:5#
```

show ssl certificate

Purpose	Used to view the SSL certificate file status on the Switch.
Syntax	**show ssl certificate**
Description	This command is used to view the SSL certificate file information currently implemented on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view certificate file information on the Switch:

```
DGS-3700-12:5#show ssl certificate
Command: show ssl certificate

Loaded with RSA Certificate!

DGS-3700-12:5#
```

download ssl certificate

Purpose	Used to download a certificate file for the SSL function on the Switch.
Syntax	**download ssl certificate <ipaddr> certfilename <path_filename 64> keyfilename <path_filename 64>**
Description	This command is used to download a certificate file for the SSL function on the Switch from a TFTP server. The certificate file is a data record used for authenticating devices on the network. It contains information on the owner, keys for authentication and digital signatures. Both the server and the client must have consistent certificate files for optimal use of the SSL function. The Switch only supports certificate files with .der file extensions.
Parameters	*<ipaddr>* – Enter the IP address of the TFTP server. *certfilename <path_filename 64>* – Enter the path and the filename of the certificate file users wish to download. *keyfilename <path_filename 64>* – Enter the path and the filename of the key exchange file users wish to download. *path_filename* – Private key file path respect to tftp server root path, and input characters max to 64 octets.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To download a certificate file and key file to the Switch:

```
DGS-3700-12:5# DGS-3700-12:5# download ssl certificate 10.55.47.1 certfilename
cert.der keyfilename pkey.der
Command: download ssl certificate 10.55.47.1 certfilename cert.der keyfilename
pkey.der

Success.

DGS-3700-12:5#
```

51

SSH COMMANDS

The steps required to use the Secure Shell (SSH) protocol for secure communication between a remote PC (the SSH Client) and the Switch (the SSH Server), are as follows:

Create a user account with admin-level access using the **create account admin <username> <password>** command. This is identical to creating any other admin-lever user account on the Switch, including specifying a password. This password is used to login to the Switch, once secure communication has been established using the SSH protocol.

Configure the user account to use a specified authorization method to identify users that are allowed to establish SSH connections with the Switch using the **config ssh authmode** command. There are three choices as to the method SSH will use to authorize the user, and they are password, publickey and hostbased.

Configure the encryption algorithm that SSH will use to encrypt and decrypt messages sent between the SSH Client and the SSH Server.

Finally, enable SSH on the Switch using the **enable ssh** command.

After following the above steps, users can configure an SSH Client on the remote PC and manage the Switch using secure, in-band communication.

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

Command	Parameters
enable ssh	
disable ssh	
config ssh authmode	[password | publickey | hostbased] [enable | disable]
show ssh authmode	
config ssh server	{maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]}(1)
show ssh server	
config ssh user	<username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr>] | password | publickey]
show ssh user authmode	
config ssh algorithm	[3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]
show ssh algorithm	

Each command is listed, in detail, in the following sections.

enable ssh

Purpose	Used to enable SSH.
Syntax	**enable ssh**
Description	This command allows users to enable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To enable SSH:

```
DGS-3700-12:5#enable ssh
Command: enable ssh

Success.

DGS-3700-12:5#
```

disable ssh

Purpose	Used to disable SSH.
Syntax	**disable ssh**
Description	This command allows users to disable SSH on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To disable SSH:

```
DGS-3700-12:5#disable ssh
Command: disable ssh

Success.

DGS-3700-12:5#
```

config ssh authmode

Purpose	Used to configure the SSH authentication mode setting.
Syntax	**config ssh authmode [password | publickey | hostbased] [enable | disable]**
Description	This command is used to configure the SSH authentication mode for users attempting to access the Switch.
Parameters	*password* – This parameter may be chosen if the administrator wishes to use a locally configured password for authentication on the Switch. *publickey* – This parameter may be chosen if the administrator wishes to use a publickey configuration set on a SSH server, for authentication. *hostbased* – This parameter may be chosen if the administrator wishes to use a host computer for authentication. This parameter is intended for Linux users requiring SSH authentication techniques and the host computer is running the Linux operating system with a SSH program previously installed. *[enable* | *disable]* – This allows users to enable or disable SSH authentication on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the SSH authentication mode by password:

```
DGS-3700-12:5#config ssh authmode password enable
Command: config ssh authmode password enable

Success.

DGS-3700-12:5#
```

show ssh authmode

Purpose	Used to display the SSH authentication mode settings.
Syntax	**show ssh authmode**
Description	This command is used to display the current SSH authentication set on the Switch.
Parameters	None.
Restrictions	None.

Example usage:

To view the current authentication mode set on the Switch:

```
DGS-3700-12:5#show ssh authmode
Command: show ssh authmode

The SSH Authmode:
-------------------------------------------------
Password    : Enabled
Publickey   : Enabled
Hostbased   : Enabled

DGS-3700-12:5#
```

config ssh server

Purpose	Used to configure the SSH server.
Syntax	**config ssh server {maxsession <int 1-8> | contimeout <sec 120-600> | authfail <int 2-20> | rekey [10min | 30min | 60min | never]}(1)**
Description	This command is used to configure the SSH server.
Parameters	*maxsession <int 1-8>* – Allows the user to set the number of users that may simultaneously access the Switch. The default setting is *8*. *contimeout <sec 120-600>* – Allows the user to set the connection timeout. The user may set a time between *120* and *600* seconds. The default is *120* seconds. *authfail <int 2-20>* – Allows the administrator to set the maximum number of attempts that a user may try to logon utilizing SSH authentication. After the maximum number of attempts is exceeded, the Switch will be disconnected and the user must reconnect to the Switch to attempt another login. *rekey [10min | 30min | 60min | never]* – Sets the time period that the Switch will change the security shell encryptions.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure the SSH server:

```
DGS-3700-12:5#config ssh server maxsession 2 contimeout 300 authfail 2
Command: config ssh server maxsession 2 contimeout 300 authfail 2

Success.

DGS-3700-12:5#
```

show ssh server

Purpose	Used to display the SSH server setting.
Syntax	**show ssh server**
Description	This command is used to display the current SSH server setting.
Parameters	None.
Restrictions	None.

Usage example:

To display the SSH server:

```
DGS-3700-12:5#show ssh server
Command: show ssh server

The SSH Server Configuration
Max Session               : 8
Connection Timeout        : 120
Authfail Attempts         : 2
Rekey Timeout             : Never

DGS-3700-12:5#
```

config ssh user

Purpose	Used to configure the SSH user.
Syntax	**config ssh user <username 15> authmode [hostbased [hostname <domain_name 32> | hostname_IP <domain_name 32> <ipaddr >] | password | publickey]**
Description	This command is used to configure the SSH user authentication method.
Parameters	*<username 15>* – Enter a username of no more than 15 characters to identify the SSH user. *authmode* – Specifies the authentication mode of the SSH user wishing to log on to the Switch. The administrator may choose between: *hostbased* – This parameter should be chosen if the user wishes to use a remote SSH server for authentication purposes. Choosing this parameter requires the user to input the following information to identify the SSH user. • *hostname <domain_name 32>* – Enter an alphanumeric string of up to 32 characters identifying the remote SSH user. • *hostname_IP <domain_name 32> <ipaddr>* – Enter the hostname and the corresponding IP address of the SSH user. *password* – This parameter should be chosen to use an administrator defined password for authentication. *publickey* – This parameter should be chosen to use the publickey on a SSH server for authentication.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the SSH user:

```
DGS-3700-12:5#config ssh user Trinity authmode password
Command: config ssh user Trinity authmode password

Success.

DGS-3700-12:5#
```

show ssh user authmode

Purpose	Used to display the SSH user setting.
Syntax	**show ssh user authmode**
Description	This command is used to display the current SSH user setting.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the SSH user:

```
DGS-3700-12:5#show ssh user authmode
Command: show ssh user authmode

Current Accounts:
Username     AuthMode   HostName        HostIP
---------   ---------  -------------   -----------
123          Password

Total Entries : 1


DGS-3700-12:5#
```

Note: To configure the SSH user, the administrator must create a user account on the Switch. For information concerning configuring a user account, please see the section of this manual entitled Basic Switch Commands and then the command, **create account**.

config ssh algorithm

Purpose	Used to configure the SSH algorithm.
Syntax	**config ssh algorithm [3DES | AES128 | AES192 | AES256 | arcfour | blowfish | cast128 | twofish128 | twofish192 | twofish256 | MD5 | SHA1 | RSA | DSA] [enable | disable]**
Description	This command is used to configure the desired type of SSH algorithm used for authentication encryption.
Parameters	*3DES* – This parameter will enable or disable the Triple_Data Encryption Standard encryption algorithm. *AES128* – This parameter will enable or disable the Advanced Encryption Standard AES128 encryption algorithm. *AES192* – This parameter will enable or disable the Advanced Encryption Standard AES192 encryption algorithm. *AES256* – This parameter will enable or disable the Advanced Encryption Standard AES256 encryption algorithm. *arcfour* – This parameter will enable or disable the Arcfour encryption algorithm. *blowfish* – This parameter will enable or disable the Blowfish encryption algorithm. *cast128* – This parameter will enable or disable the Cast128 encryption algorithm. *twofish128* – This parameter will enable or disable the twofish128 encryption algorithm. *twofish192* – This parameter will enable or disable the twofish192 encryption algorithm. *MD5* – This parameter will enable or disable the MD5 Message Digest encryption algorithm. *SHA1* – This parameter will enable or disable the Secure Hash Algorithm encryption. *RSA* – This parameter will enable or disable the RSA encryption algorithm. *DSA* – This parameter will enable or disable the Digital Signature Algorithm encryption. *[enable | disable]* – This allows the user to enable or disable algorithms entered in this command, on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Usage example:

To configure SSH algorithm:

```
DGS-3700-12:5#config ssh algorithm blowfish enable
Command: config ssh algorithm blowfish enable

Success.

DGS-3700-12:5#
```

show ssh algorithm

Purpose	Used to display the SSH algorithm setting.
Syntax	**show ssh algorithm**
Description	This command is used to display the current SSH algorithm setting status.
Parameters	None.
Restrictions	None.

Usage Example:

To display SSH algorithms currently set on the Switch:

```
DGS-3700-12:5#show ssh algorithm
Command: show ssh algorithm

Encryption Algorithm
--------------------------
3DES       : Enabled
AES128     : Enabled
AES192     : Enabled
AES256     : Enabled
Arcfour    : Enabled
Blowfish   : Enabled
Cast128    : Enabled
Twofish128 : Enabled
Twofish192 : Enabled
Twofish256 : Enabled

Data Integrity Algorithm
--------------------------
MD5        : Enabled
SHA1       : Enabled

Public Key Algorithm
--------------------------
RSA        : Enabled
DSA        : Enabled

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

52

ACCESS AUTHENTICATION CONTROL COMMANDS

The TACACS / XTACACS / TACACS+ / RADIUS commands allows secure access to the Switch using the TACACS / XTACACS / TACACS+ / RADIUS protocols. When a user logs in to the Switch or tries to access the administrator level privilege, he or she is prompted for a password. If TACACS / XTACACS / TACACS+ / RADIUS authentication is enabled on the Switch, it will contact a TACACS / XTACACS / TACACS+ / RADIUS server to verify the user. If the user is verified, he or she is granted access to the Switch.

There are currently three versions of the TACACS security protocol, each a separate entity. The Switch's software supports the following versions of TACACS:

- TACACS (Terminal Access Controller Access Control System) —Provides password checking and authentication, and notification of user actions for security purposes utilizing via one or more centralized TACACS servers, utilizing the UDP protocol for packet transmission.
- Extended TACACS (XTACACS) — An extension of the TACACS protocol with the ability to provide more types of authentication requests and more types of response codes than TACACS. This protocol also uses UDP to transmit packets.
- TACACS+ (Terminal Access Controller Access Control System plus) — Provides detailed access control for authentication for network devices. TACACS+ is facilitated through Authentication commands via one or more centralized servers. The TACACS+ protocol encrypts all traffic between the Switch and the TACACS+ daemon, using the TCP protocol to ensure reliable delivery.

The Switch also supports the RADIUS protocol for authentication using the Access Authentication Control commands. RADIUS or Remote Authentication Dial In User Server also uses a remote server for authentication and can be responsible for receiving user connection requests, authenticating the user and returning all configuration information necessary for the client to deliver service through the user. RADIUS may be facilitated on this Switch using the commands listed in this section.

In order for the TACACS / XTACACS / TACACS+ / RADIUS security function to work properly, a TACACS / XTACACS / TACACS+ / RADIUS server must be configured on a device other than the Switch, called a server host and it must include usernames and passwords for authentication. When the user is prompted by the Switch to enter usernames and passwords for authentication, the Switch contacts the TACACS / XTACACS / TACACS+ / RADIUS server to verify, and the server will respond with one of three messages:

A) The server verifies the username and password, and the user is granted normal user privileges on the Switch.

B) The server will not accept the username and password and the user is denied access to the Switch.

C) The server doesn't respond to the verification query. At this point, the Switch receives the timeout from the server and then moves to the next method of verification configured in the method list.

The Switch has four built-in server groups, one for each of the TACACS, XTACACS, TACACS+ and RADIUS protocols. These built-in server groups are used to authenticate users trying to access the Switch. The users will set server hosts in a preferable order in the built-in server group and when a user tries to gain access to the Switch, the Switch will ask the first server host for authentication. If no authentication is made, the second server host in the list will be queried, and so on. The built-in server group can only have hosts that are running the specified protocol. For example, the TACACS server group can only have TACACS server hosts.

The administrator for the Switch may set up five different authentication techniques per user-defined method list (TACACS / XTACACS / TACACS+ / RADIUS / local / none) for authentication. These techniques will be listed in an order preferable, and defined by the user for normal user authentication on the Switch, and may contain up to eight authentication techniques. When a user attempts to access the Switch, the Switch will select the first technique listed for authentication. If the first technique goes through its *server hosts* and no authentication is returned, the Switch will then go to the next technique listed in the server group for authentication, until the authentication has been verified or denied, or the list is exhausted.

Please note that user granted access to the Switch will be granted normal user privileges on the Switch. To gain access to admin level privileges, the user must enter the **enable admin** command, which is only available for logining in the Switch from the three versions of the TACACS server, and then enter a password, which was previously configured by the administrator of the Switch.

NOTE: TACACS, XTACACS and TACACS+ are separate entities and are not compatible. The Switch and the server must be configured exactly the same, using the same protocol. (For example, if the Switch is set up for TACACS authentication, so must be the host server.)

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

Command	Parameters
enable authen_policy	
disable authen_policy	
show authen_policy	
create authen_login method_list_name	<string 15>
config authen_login	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}(1)
delete authen_login method_list_name	<string 15>
show authen_login	[default | method_list_name <string 15> | all]
create authen_enable method_list_name	<string 15>
config authen_enable	[default | method_list_name <string 15>] method {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}(1)
delete authen_enable method_list_name	<string 15>
show authen_enable	[default | method_list_name <string 15> | all]
config authen application	[console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]
show authen application	
create authen server_group	<string 15>
config authen server_group	[tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
delete authen server_group	<string 15>
show authen server_group	{<string 15>}
create authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}
config authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit <int 1-255>}(1)
delete authen server_host	<ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]
show authen server_host	
config authen parameter response_timeout	<int 0-255>
config authen parameter attempt	<int 1-255>
show authen parameter	
enable admin	
config admin local_enable	

Each command is listed, in detail, in the following sections.

enable authen_policy

Purpose	Used to enable system access authentication policy.
Syntax	**enable authen_policy**
Description	This command will enable an administrator-defined authentication policy for users trying to access the Switch. When enabled, the device will check the method list and choose a technique for user authentication upon login.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To enable the system access authentication policy:

```
DGS-3700-12:5#enable authen_policy
Command: enable authen_policy

Success.

DGS-3700-12:5#
```

disable authen_policy

Purpose	Used to disable system access authentication policy.
Syntax	**disable authen_policy**
Description	This command will disable the administrator-defined authentication policy for users trying to access the Switch. When disabled, the Switch will access the local user account database for username and password verification. In addition, the Switch will now accept the local enable password as the authentication for normal users attempting to access administrator level privileges.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To disable the system access authentication policy:

```
DGS-3700-12:5#disable authen_policy
Command: disable authen_policy

Success.

DGS-3700-12:5#
```

show authen_policy

Purpose	Used to display the system access authentication policy status on the Switch.
Syntax	**show authen_policy**
Description	This command will show the current status of the access authentication policy on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the system access authentication policy:

```
DGS-3700-12:5#show authen_policy
Command: show authen_policy

Authentication Policy: Enabled

DGS-3700-12:5#
```

create authen_login method_list_name

Purpose	Used to create a user defined method list of authentication methods for users logging on to the Switch.
Syntax	**create authen_login method_list_name <string 15>**
Description	This command is used to create a list for 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>* – Enter an alphanumeric string of up to 15 characters to define the given *method list*.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the method list "Trinity.":

```
DGS-3700-12:5#create authen_login method_list_name Trinity
Command: create authen_login method_list_name Trinity

Success.

DGS-3700-12:5#
```

config authen_login

Purpose	Used 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 {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local | none}(1)**
Description	This command is used to configure 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 will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local,* the Switch will send an authentication request to the first *tacacs* host in the server group. If no response comes from the server host, the Switch will send an authentication request to the second *tacacs* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local* account database set in the Switch is used to authenticate the user. When the local method is used, the privilege level will be dependant on the local account privilege configured on the Switch. Successful login using any of these methods will give the user a "user" privilege 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 a combination of up to four of the following authentication methods:

config authen_login

- *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list.
- *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list.
- *server_group <string 15>* – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.
- *local* – Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch.
- *none* – Adding this parameter will require no authentication to access the Switch.

method_list_name – Enter a previously implemented method list name defined by the user. The user may add one, or a combination of up to four of the following authentication methods to this method list:

- *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from a remote TACACS server.
- *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from a remote XTACACS server.
- *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from a remote TACACS+ server.
- *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from a remote RADIUS server.
- *server_group <string 15>* – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch.
- *local* – Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch.
- *none* – Adding this parameter will require no authentication to access the Switch.

NOTE: Entering *none* or *local* as an authentication protocol will override any other authentication that follows it on a method list or on the default method list.

Restrictions Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list “Trinity” with authentication methods TACACS, XTACACS and local, in that order.

```
DGS-3700-12:5#config authen_login method_list_name Trinity method tacacs xtacacs local
Command: config authen_login method_list_name Trinity method tacacs xtacacs local

Success.

DGS-3700-12:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DGS-3700-12:5#config authen_login default method xtacacs tacacs+ local
Command: config authen_login default method xtacacs tacacs+ local

Success.

DGS-3700-12:5#
```

delete authen_login method_list_name

Purpose	Used to delete a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**delete authen_login method_list_name <string 15>**
Description	This command is used to delete a list for authentication methods for user login.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the method list name “Trinity”:

```
DGS-3700-12:5#delete authen_login method_list_name Trinity
Command: delete authen_login method_list_name Trinity

Success.

DGS-3700-12:5#
```

show authen_login

Purpose	Used to display a previously configured user defined method list of authentication methods for users logging on to the Switch.
Syntax	**show authen_login [default | method_list_name <string 15> | all]**
Description	This command is used to show a list of authentication methods for user login.
Parameters	*default* – Entering this parameter will display the default method list for users logging on to the Switch. *method_list_name <string 15>* – Enter an alphanumeric string of up to 15 characters to define the given method list to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: • *Method List Name* – The name of a previously configured method list name. • *Priority* – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). • *Method Name* – Defines which security protocols are implemented, per method list name. • *Comment* – Defines the type of Method. *User-defined Group* refers to server group defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS / XTACACS / TACACS+ / RADIUS which are local (authentication through the user account on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the authentication login method list named Trinity:

```
DGS-3700-12:5#show authen_login method_list_name Trinity
Command: show authen_login method_list_name Trinity

Method List Name  Priority    Method Name      Comment
---------------- --------    -------------   ---------
Trinity              1        tacacs+          Built-in Group
                     2        tacacs           Built-in Group
                     3        Darren           User-defined Group
                     4        local            Keyword

DGS-3700-12:5#
```

create authen_enable method_list_name

Purpose	Used 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	This command is used to promote 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 enable method lists can be implemented on the Switch.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to create.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a user-defined method list, named "Permit" for promoting user privileges to Administrator privileges:

```
DGS-3700-12:5#create authen_enable method_list_name Permit
Command: create authen_enable method_list_name Permit

Success.

DGS-3700-12:5#
```

config authen_enable

Purpose	Used 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 {tacacs | xtacacs | tacacs+ | radius | server_group <string 15> | local_enable | none}(1)**
Description	This command is used to promote 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 enable method lists can be implemented simultaneously on the Switch. The sequence of methods implemented in this command will affect the authentication result. For example, if a user enters a sequence of methods like *tacacs – xtacacs – local_enable,* the Switch will send an authentication request to the first *TACACS* host in the server group. If no verification is found, the Switch will send an authentication request to the second *TACACS* host in the server group and so on, until the list is exhausted. At that point, the Switch will restart the same sequence with the following protocol listed, *xtacacs*. If no authentication takes place using the *xtacacs* list, the *local_enable* password set in the Switch is used to authenticate the user. Successful authentication using any of these methods will give the user an "Admin" level privilege.
Parameters	*default* – The default method list for administration rights authentication, as defined by the user. The user may choose one or a combination of up to four (4) of the following authentication methods: • *tacacs* – Adding this parameter will require the user to be authenticated using the *TACACS* protocol from the remote TACACS *server hosts* of the TACACS *server group* list. • *xtacacs* – Adding this parameter will require the user to be authenticated using the *XTACACS* protocol from the remote XTACACS *server hosts* of the XTACACS *server group* list. • *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from the remote TACACS+ *server hosts* of the TACACS+ *server group* list. • *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from the remote RADIUS *server hosts* of the RADIUS *server group* list. • *server_group <string 15>* – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. • *local_enable* – Adding this parameter will require the user to be authenticated using the local *user account* database on the Switch. • *none* – Adding this parameter will require no authentication to access the Switch. *method_list_name* – Enter a previously implemented method list name defined by the user (**create authen_enable**). The user may add one, or a combination of up to four (4) of the following authentication methods to this method list: • *tacacs* – Adding this parameter will require the user to be authenticated using the

config authen_enable

	TACACS protocol from a remote TACACS server. • *xtacacs* – Adding this parameter will require the user to be authenticated using the XTACACS protocol from a remote XTACACS server. • *tacacs+* – Adding this parameter will require the user to be authenticated using the *TACACS+* protocol from a remote TACACS+ server. • *radius* – Adding this parameter will require the user to be authenticated using the *RADIUS* protocol from a remote RADIUS server. • *server_group* <*string 15*> – Adding this parameter will require the user to be authenticated using a user-defined server group previously configured on the Switch. • *local_enable* – Adding this parameter will require the user 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. • *none* – Adding this parameter will require no authentication to access the administration level privileges on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the user defined method list "Permit" with authentication methods TACACS, XTACACS and local, in that order.

```
DGS-3700-12:5#config authen_enable method_list_name Trinity method tacacs xtacacs
local
Command: config authen_enable method_list_name Trinity method tacacs xtacacs local

Success.

DGS-3700-12:5#
```

Example usage:

To configure the default method list with authentication methods XTACACS, TACACS+ and local, in that order:

```
DGS-3700-12:5#config authen_enable default method xtacacs tacacs+ local
Command: config authen_enable default method xtacacs tacacs+ local

Success.

DGS-3700-12:5#
```

delete authen_enable method_list_name

Purpose	Used to delete a user-defined method 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	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	<*string 15*> – Enter an alphanumeric string of up to 15 characters to define the given *enable method list* to delete.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the user-defined method list "Permit"

```
DGS-3700-12:5#delete authen_enable method_list_name Permit
Command: delete authen_enable method_list_name Permit

Success.

DGS-3700-12:5#
```

show authen_enable

Purpose	Used to display the method list of authentication methods for promoting normal user level privileges to Administrator level privileges on the Switch.
Syntax	**show authen_enable [default | method_list_name <string 15> | all]**
Description	This command is used to delete a user-defined method list of authentication methods for promoting user level privileges to Administrator level privileges.
Parameters	*default* – Entering this parameter will display the default method list for users attempting to gain access to Administrator level privileges on the Switch. *method_list_name <string 15>* – Enter an alphanumeric string of up to 15 characters to define the given *method list* the user wishes to view. *all* – Entering this parameter will display all the authentication login methods currently configured on the Switch. The window will display the following parameters: • *Method List Name* – The name of a previously configured method list name. • *Priority* – Defines which order the method list protocols will be queried for authentication when a user attempts to log on to the Switch. Priority ranges from 1(highest) to 4 (lowest). • *Method Name* – Defines which security protocols are implemented, per method list name. • *Comment* – Defines the type of Method. *User-defined Group* refers to *server groups* defined by the user. *Built-in Group* refers to the TACACS, XTACACS, TACACS+ and RADIUS security protocols which are permanently set in the Switch. *Keyword* refers to authentication using a technique INSTEAD of TACACS/XTACACS/TACACS+/RADIUS which are local (authentication through the *local_enable* password on the Switch) and none (no authentication necessary to access any function on the Switch).
Restrictions	None.

Example usage:

To display all method lists for promoting user level privileges to administrator level privileges.

```
DGS-3700-12:5#show authen_enable all
Command: show authen_enable all

Method List Name  Priority   Method Name       Comment
----------------  --------   ---------------   ------------------
Permit               1        tacacs+           Built-in Group
                     2        tacacs            Built-in Group
                     3        Darren            User-defined Group
                     4        local             Keyword

default              1        tacacs+           Built-in Group
                     2        local             Keyword

Total Entries : 2

DGS-3700-12:5#
```

config authen application

Purpose	Used to configure various applications on the Switch for authentication using a previously configured method list.
Syntax	**config authen application [console | telnet | ssh | http | all] [login | enable] [default | method_list_name <string 15>]**
Description	This command is used to configure Switch configuration applications (console, telnet, ssh, web) for login at the user level and at the administration level (*authen_enable*) utilizing a previously configured method list.
Parameters	*application* – Choose the application to configure. The user may choose one of the following five options to configure. • *console* – Choose this parameter to configure the command line interface login method. • *telnet* – Choose this parameter to configure the telnet login method. • *ssh* – Choose this parameter to configure the Secure Shell login method. • *http* – Choose this parameter to configure the web interface login method. • *all* – Choose this parameter to configure all applications (console, telnet, ssh, web) login method. *login* – Use this parameter to configure an application for normal login on the user level, using a previously configured method list. *enable* – Use this parameter to configure an application for upgrading a normal user level to administrator privileges, using a previously configured method list. *default* – Use this parameter to configure an application for user authentication using the default method list. *method_list_name <string 15>* – Use this parameter to configure an application for user authentication using a previously configured method list. Enter a alphanumeric string of up to 15 characters to define a previously configured method list.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the default method list for the web interface:

```
DGS-3700-12:5#config authen application http login default
Command: config authen application http login default

Success.

DGS-3700-12:5#
```

show authen application

Purpose	Used to display authentication methods for the various applications on the Switch.
Syntax	**show authen application**
Description	This command will display all of the authentication method lists (login, enable administrator privileges) for Switch configuration applications (console, telnet, SSH, web) currently configured on the Switch.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the login and enable method list for all applications on the Switch:

```
DGS-3700-12:5#show authen application
Command: show authen application

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

DGS-3700-12:5#
```

create authen server_host

Purpose	Used to create an authentication server host.
Syntax	**create authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit < 1-255>}**
Description	This command will create an authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host to add. *protocol* – The protocol used by the server host. The user may choose one of the following: • *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. • *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. • *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. • *radius* – Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* – Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1812* and *1813* for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters. *timeout <int 1-255>* – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds. *retransmit <int 1-255>* – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create a TACACS+ authentication server host, with port number 1234, a timeout value of 10 seconds and a retransmit count of 5.

```
DGS-3700-12:5#create authen server_host 10.1.1.121 protocol tacacs+ port 1234
timeout 10 retransmit 5
Command: create authen server_host 10.1.1.121 protocol tacacs+ port 1234 timeout 10
retransmit 5

Success.

DGS-3700-12:5#
```

config authen server_host

Purpose	Used to configure a user-defined authentication server host.
Syntax	**config authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius] {port <int 1-65535> | key [<key_string 254> | none] | timeout <int 1-255> | retransmit < 1-255>}(1)**
Description	This command will configure a user-defined authentication server host for the TACACS/XTACACS/TACACS+/RADIUS security protocols on the Switch. When a user attempts to access the Switch with the authentication protocol enabled, the Switch will send authentication packets to a remote TACACS/XTACACS/TACACS+/RADIUS server host on a remote host. The TACACS/XTACACS/TACACS+/RADIUS server host will then verify or deny the request and return the appropriate message to the Switch. More than one authentication protocol can be run on the same physical server host but, remember that TACACS/XTACACS/TACACS+/RADIUS are separate entities and are not compatible with each other. The maximum supported number of server hosts is 16.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host the user wishes to alter. *protocol* – The protocol used by the server host. The user may choose one of the following: • *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. • *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. • *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. • radius – Enter this parameter if the server host utilizes the RADIUS protocol. *port <int 1-65535>* – Enter a number between *1* and *65535* to define the virtual port number of the authentication protocol on a server host. The default port number is *49* for TACACS/XTACACS/TACACS+ servers and *1812* and *1813* for RADIUS servers but the user may set a unique port number for higher security. *key <key_string 254>* – Authentication key to be shared with a configured TACACS+ or RADIUS server only. Specify an alphanumeric string up to 254 characters or choose none. *timeout <int 1-255>* – Enter the time in seconds the Switch will wait for the server host to reply to an authentication request. The default value is *5* seconds. *retransmit <int 1-255>* – Enter the value in the retransmit field to change how many times the device will resend an authentication request when the server does not respond. This field is inoperable for the TACACS+ protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure a TACACS+ authentication server host, with port number 4321, a timeout value of 12 seconds and a retransmit count of 4.

```
DGS-3700-12:5#config authen server_host 10.1.1.121 protocol tacacs+ port 4321
timeout 12 retransmit 4
Command: config authen server_host 10.1.1.121 protocol tacacs+ port 4321 timeout 12
retransmit 4

Success.

DGS-3700-12:5#
```

delete authen server_host

Purpose	Used to delete a user-defined authentication server host.
Syntax	**delete authen server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command is used to delete a user-defined authentication server host previously created on the Switch.
Parameters	*server_host <ipaddr>* – The IP address of the remote server host to be deleted. *protocol* – The protocol used by the server host the user wishes to delete. The user may choose one of the following: • *tacacs* – Enter this parameter if the server host utilizes the TACACS protocol. • *xtacacs* – Enter this parameter if the server host utilizes the XTACACS protocol. • *tacacs+* – Enter this parameter if the server host utilizes the TACACS+ protocol. • *radius* – Enter this parameter if the server host utilizes the RADIUS protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete a user-defined TACACS+ authentication server host:

```
DGS-3700-12:5#delete authen server_host 10.1.1.121 protocol tacacs+
Command: delete authen server_host 10.1.1.121 protocol tacacs+

Success.

DGS-3700-12:5#
```

show authen server_host

Purpose	Used to view a user-defined authentication server host.
Syntax	**show authen server_host**
Description	This command is used to view user-defined authentication server hosts previously created on the Switch. The following parameters are displayed: *IP Address* – The IP address of the authentication server host. *Protocol* – The protocol used by the server host. Possible results will include TACACS, XTACACS, TACACS+ or RADIUS. *Port* – The virtual port number on the server host. The default value is *49*. *Timeout* – The time in seconds the Switch will wait for the server host to reply to an authentication request. *Retransmit* – The value in the retransmit field denotes how many times the device will resend an authentication request when the TACACS server does not respond. This field is inoperable for the tacacs+ protocol. *Key* – Authentication key to be shared with a configured TACACS+ server only.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authentication server hosts currently set on the Switch:

```
DGS-3700-12:5#show authen server_host
Command: show authen server_host

IP Address    Protocol    Port  Timeout  Retransmit  Key
-----------   --------    ----- -------  ----------  -----
10.53.13.94    TACACS     49       5         2       No Use

Total Entries : 1

DGS-3700-12:5#
```

create authen server_group

Purpose	Used to create a user-defined authentication server group.
Syntax	**create authen server_group {<string 15>}**
Description	This command will create an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may add up to eight authentication server hosts to this group using the **config authen server_group** command.
Parameters	*<string 15>* – Enter an alphanumeric string of up to 15 characters to define the newly created server group.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To create the server group “group_1”:

```
DGS-3700-12:5#create authen server_group group_1
Command: create authen server_group group_1

Success.

DGS-3700-12:5#
```

config authen server_group

Purpose	Used to configure a user-defined authentication server group.
Syntax	**config authen server_group [tacacs | xtacacs | tacacs+ | radius | <string 15>] [add | delete] server_host <ipaddr> protocol [tacacs | xtacacs | tacacs+ | radius]**
Description	This command will configure an authentication server group. A server group is a technique used to group TACACS/XTACACS/TACACS+/RADIUS server hosts into user defined categories for authentication using method lists. The user may define the type of server group by protocol or by previously defined server group. Up to eight authentication server hosts may be added to any particular group
Parameters	*server_group* – The user may define the group by protocol groups built into the Switch (TACACS/XTACACS/TACACS+/RADIUS), or by a user-defined group previously created using the **create authen server_group** command. • *tacacs* – Use this parameter to utilize the built-in TACACS server protocol on the Switch. Only server hosts utilizing the TACACS protocol may be added to this group. • *xtacacs* – Use this parameter to utilize the built-in XTACACS server protocol on the Switch. Only server hosts utilizing the XTACACS protocol may be added to this group. • *tacacs+* – Use this parameter to utilize the built-in TACACS+ server protocol on the Switch. Only server hosts utilizing the TACACS+ protocol may be added to this group. • *radius* – Use this parameter to utilize the built-in RADIUS server protocol on the Switch. Only server hosts utilizing the RADIUS protocol may be added to this group. • <*string 15*> – Enter an alphanumeric string of up to 15 characters to define the previously created server group. This group may add any combination of server hosts to it, regardless of protocol. *add/delete* – Enter the correct parameter to add or delete a server host from a server group. *server_host* <*ipaddr*> – Enter the IP address of the previously configured server host to add or delete. *protocol* – Enter the protocol utilized by the server host. There are three options: • *tacacs* – Use this parameter to define the protocol if the server host is using the TACACS authentication protocol. • *xtacacs* – Use this parameter to define the protocol if the server host is using the XTACACS authentication protocol. • *tacacs+* – Use this parameter to define the protocol if the server host is using the TACACS+ authentication protocol. • *radius* – Use this parameter to define the protocol if the server host is using the RADIUS authentication protocol.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To add an authentication host to server group “group_1”:

```
DGS-3700-12:5# config authen server_group group_1 add server_host 10.1.1.121
protocol tacacs+
Command: config authen server_group group_1 add server_host 10.1.1.121 protocol
tacacs+

Success.

DGS-3700-12:5#
```

delete authen server_group

Purpose	Used to delete a user-defined authentication server group.
Syntax	**delete authen server_group <string 15>**
Description	This command will delete an authentication server group.
Parameters	<*string 15*> – Enter an alphanumeric string of up to 15 characters to define the previously created server group to be deleted.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To delete the server group "group_1":

```
DGS-3700-12:5#delete server_group group_1
Command: delete server_group group_1

Success.

DGS-3700-12:5#
```

show authen server_group

Purpose	Used to view authentication server groups on the Switch.
Syntax	**show authen server_group {<string 15>}**
Description	This command will display authentication server groups currently configured on the Switch. This command will display the following fields: Group Name: The name of the server group currently configured on the Switch, including built in groups and user defined groups. IP Address: The IP address of the server host. Protocol: The authentication protocol used by the server host.
Parameters	<*string 15*> – Enter an alphanumeric string of up to 15 characters to define the previously created server group to be viewed. Entering this command without the <*string*> parameter will display all authentication server groups on the Switch.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view authentication server groups currently set on the Switch.

```
DGS-3700-12:5#show authen server_group
Command: show authen server_group

Server Group : mix_1

Group Name       IP Address      Protocol
---------------  --------------  --------
mix_1             10.1.1.222     TACACS+
                  10.1.1.223     TACACS
radius            10.1.1.224     RADIUS
tacacs            10.1.1.225     TACACS
tacacs+           10.1.1.226     TACACS+
xtacacs           10.1.1.227     XTACACS

Total Entries : 5

DGS-3700-12:5#
```

config authen parameter response_timeout

Purpose	Used to configure the amount of time the Switch will wait for a user to enter authentication before timing out.
Syntax	**config authen parameter response_timeout <int 0-255>**
Description	This command will set the time the Switch will wait for a response of authentication from the user.
Parameters	*response_timeout <int 0-255>* – Set the time, in seconds, the Switch will wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. Zero means there won't be a time-out. The default value is *0* seconds.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the response timeout for 60 seconds:

```
DGS-3700-12:5# config authen parameter response_timeout 60
Command: config authen parameter response_timeout 60

Success.

DGS-3700-12:5#
```

config authen parameter attempt

Purpose	Used to configure the maximum number of times the Switch will accept authentication attempts.
Syntax	**config authen parameter attempt <int 1-255>**
Description	This command will configure the maximum number of times the Switch will accept authentication attempts. Users failing to be authenticated after the set amount of attempts will be denied access to the Switch and will be locked out of further authentication attempts. Command line interface users will have to wait 60 seconds before another authentication attempt. Telnet users will be disconnected from the Switch.
Parameters	*parameter attempt <int 1-255>* – Set the maximum number of attempts the user may try to become authenticated by the Switch, before being locked out. The default setting is *3.*
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To set the maximum number of authentication attempts at 5:

```
DGS-3700-12:5# config authen parameter attempt 5
Command: config authen parameter attempt 5

Success.

DGS-3700-12:5#
```

show authen parameter

Purpose	Used to display the authentication parameters currently configured on the Switch.
Syntax	**show authen parameter**
Description	This command will display the authentication parameters currently configured on the Switch, including the response timeout and user authentication attempts. This command will display the following fields: Response timeout – The configured time allotted for the Switch to wait for a response of authentication from the user attempting to log in from the command line interface or telnet interface. User attempts: The maximum number of attempts the user may try to become authenticated by the Switch, before being locked out.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To view the authentication parameters currently set on the Switch:

```
DGS-3700-12:5#show authen parameter
Command: show authen parameter

Response Timeout : 30 seconds
User Attempts    : 3

DGS-3700-12:5#
```

enable admin

Purpose	Used to promote user level privileges to administrator level privileges.
Syntax	**enable admin**
Description	This command is for users who have logged on to the Switch on the normal user level, to become promoted to the administrator level. After logging on to the Switch users will have only user level privileges. To gain access to administrator level privileges, the user will enter this command and will have to enter an authentication password. Possible authentication methods for this function include TACACS, XTACACS, TACACS+, RADIUS, user defined server groups, local enable (local account on the Switch), or no authentication (*none*). Because XTACACS and TACACS do 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	None.

Example usage:

To enable administrator privileges on the Switch:

```
DGS-3700-12:5#enable admin
Password: ******

DGS-3700-12:5#
```

config admin local_enable

Purpose	Used to configure the local enable password for administrator level privileges.
Syntax	**config admin local_enable**
Description	This command will configure the locally enabled password for the **enable admin** command. When a user chooses the **local_enable** method to promote user level privileges to administrator privileges, he or she will be prompted to enter the password configured here that is set locally on the Switch.
Parameters	*<password 15>* – After entering this command, the user will be prompted to enter the old password, then a new password in an alphanumeric string of no more than 15 characters, and finally prompted to enter the new password again for confirmation. See the example below.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To configure the password for the "local_enable" authentication method.

```
DGS-3700-12:5#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-3700-12:5#
```

53

MAC-BASED ACCESS CONTROL COMMANDS LIST

The MAC-based Access Control Commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable mac_based_access_control	
disable mac_based_access_control	
config mac_based_access_control password	<passwd 16>
config mac_based_access_control method	[local | radius]
config mac_based_access_control ports	[<portlist> | all] {state [enable | disable] | mode [port_based | host_based] |aging_time [infinite|<min 1-1440>] | hold_time [infinite|<sec 1-300>]}(1)
config mac_based_access_control guest_vlan ports	<portlist>
create mac_based_access_control	[guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
delete mac_based_access_control	[guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
create mac_based_access_control_local	mac <macaddr> [vlan < vlan_name 32> | vlanid <vlanid 1-4094>]
config mac_based_access_control_local	mac <macaddr> [vlan <vlan_name 32>| vlanid <vlanid 1-4094>]
delete mac_based_access_control_local	[mac <macaddr> |vlan < vlan_name 32> | vlanid <vlanid 1-4094>]
show mac_based_access_control	{ports [<portlist> | all]}
show mac_based_access_control_local	{[mac <macaddr>|vlan<vlan_name 32>|vlanid <vlanid 1-4094>]}
show mac_based_access_control auth_mac	{ports <portlist>}
clear mac_based_access_control auth_mac	[ports [all | <portlist>] | mac_addr <macaddr>]

Each command is listed, in detail, in the following sections.

enable mac_based_access_control

Purpose	Used to enable MAC-based Access Control.
Syntax	**enable mac_based_access_control**
Description	This command is used to enable the MAC-based Access Control function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable MAC-based access control:

```
DGS-3700-12:5#enable mac_based_access_control
Command: enable mac_based_access_control

Success.

DGS-3700-12:5#
```

disable mac_based_access_control

Purpose	Used to disable MAC-based Access Control.
Syntax	**disable mac_based_access_control**
Description	This command is used to disable the MAC-based Access Control function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable mac_based_access_control:

```
DGS-3700-12:5#disable mac_based_access_control
Command: disable mac_based_access_control

Success.

DGS-3700-12:5#
```

config mac_based_access_control password

Purpose	Used to configure the password of the MAC-based Access Control.
Syntax	**config mac_based_access_control password < passwd 16>**
Description	This command will set the password that will be used for authentication via RADIUS server.
Parameters	*<passwd 16>* – In RADIUS mode, the switch communicate with RADIUS server use the password. The maximum length of the key is 16.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config the MAC-based access control password:

```
DGS-3700-12:5#config mac_based_access_control password 123
Command: config mac_based_access_control password 123

Success.

DGS-3700-12:5#
```

config mac_based_access_control method

Purpose	Used to configure the mac_based_access_control authenticating method
Syntax	**config mac_based_access_control method [local | radius]**
Description	This command is used to specify to authenticate via local database or via RADIUS server.
Parameters	*local* – Specifies to authenticate via local database. *radius* – Specifies to authenticate via RADIUS server.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To config mac_based_access_control method:

```
DGS-3700-12:5#config mac_based_access_control method local
Command: config mac_based_access_control method local

Success.

DGS-3700-12:5#
```

config mac_based_access_control ports

Purpose	Used to configure the parameter of the MAC-Based Access Control.
Syntax	**config mac_based_access_control ports [<portlist> | all] {state [enable | disable] | mode [port_based | host_based] |aging_time [infinite|<min 1-1440>] | hold_time [infinite|<sec 1-300>]}(1)**
Description	This command is used to configure MAC-Based Access Control setting. If a port is a member of guest VLAN, it only can access either guest VLAN (unauthenticated) or target VLAN /administrative PVID VLAN (authenticated), the original 802.1Q VLAN configuration will not take effect. For MAC_based_access_control enabled port, after enabling the Guest VLAN, it will be removed from all static 1Q VLANs and added to the guest VLAN's untagged member, the port's PVID will be changed to Guest VLAN VID. If the guest VLAN is disabled, the switch will restore the original 802.1Q VLANs for the port and change PVID to administrative PVID.
Parameters	*ports* – A range of ports enable or disable mac_based_access_control function. *state* – Specify whether MAC_based_access_control function is enabled or disabled. *mode* – Either port_based or host_based. • Port_based mode: In this mode, if one of the attached hosts is successfully authorized, all hosts on the same port will be granted access to the network. If the port authorization fails, this port will continue authenticating. • Host_based mode: In this mode, every user can individually authenticate and access the network. *aging_time* – A time period during which an authenticated host will be kept in authenticated state. When the aging time is time-out, the host will be moved back to unauthenticated state. *hold_time* – If a host fails to pass the authentication, the next authentication will not start within hold_time unless the user clear the entry state manually.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To config mac_based_access_control port state:

```
DGS-3700-12:5#config mac_based_access_control ports 1-8 state enable
Command: config mac_based_access_control ports 1-8 state enable

Success.

DGS-3700-12:5#
```

config mac_based_access_control guest_vlan ports

Purpose	Used to config the mac_based_access_control guest_vlan membership
Syntax	**config mac_based_access_control guest_vlan ports <portlist>**
Description	This command put the specified port in guest-vlan mode. For those ports not contained in the portlist, they are in non-guest VLAN mode.For detailed information for operation of guest VLAN mode, please see the description for config mac based_access_control port command.
Parameters	*<portlist>* – When the guest VLAN is configured for a port, the guest VLAN will be enabled, only after MAC_based_access_control and global are both enabled on the same port. This port will be added to the guest VLAN as an untagged member and can access this guest VLAN before being authenticated.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To config mac_based_access_control port guest_vlan:

```
DGS-3700-12G:5#config mac_based_access_control guest_vlan ports 1
Command: config mac_based_access_control guest_vlan ports 1

Success.

DGS-3700-12G:5#
```

create mac_based_access_control guest_vlan

Purpose	Used to assign the guest VLAN.
Syntax	**create mac_based_access_control [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]**
Description	This command is used to assign the guest VLAN.
Parameters	*guest_vlan* – If the MAC address is authorized, the port will be assigned to this VLAN. *guest_vlanid* – guest VLAN ID, if the MAC address is authorized, the port will be assigned to this vlan.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create MAC-based access control guest VLAN:

```
DGS-3700-12:5#create mac_based_access_control_guest vlan default
Command: create mac_based_access_control_guest vlan default

Success.

DGS-3700-12:5#
```

delete mac_based_access_control guest_vlan

Purpose	Used to de-assign the guest VLAN.
Syntax	**delete mac_based_access_control** [guest_vlan <vlan_name 32> | guest_vlanid <vlanid 1-4094>]
Description	This command is used to de-assign the guest VLAN. When the guest VLAN is de-assigned, the guest VLAN function is disabled.
Parameters	*guest_vlan* – Specifies the name of the guest VLAN. *guest_vlanid* – Specifies the id of the guest VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To de-assign a guest VLAN:

```
DGS-3700-12:5#delete mac_based_access_control guest_vlan default
Command: delete mac_based_access_control_guest_vlan default

Success.

DGS-3700-12:5#
```

create mac_based_access_control_local

Purpose	Used to create the local database entry.
Syntax	**create mac_based_access_control_local mac <macaddr> [vlan < vlan_name 32> | vlanid <vlanid 1-4094>]**
Description	This command is used to create a database entry.
Parameters	*mac* – The MAC address that accepts access by local mode. *vlan* – If the MAC address is authorized, the port will be assigbed to this VLAN. *vlanid* <*vlanid 1-4094*> – the vlan id of specified VLAN,the range of the VLAN ID is from 1 to 4094. If the MAC address is authorized, the port will be assigned to this VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create MAC-based access control local:

```
DGS-3700-12:5#create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default
Command: create mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3700-12:5#
```

config mac_based_access_control_local

Purpose	Used to config the local database entry.
Syntax	**config mac_based_access_control_local mac <macaddr> [vlan < vlan_name 32> | vlanid <vlanid 1-4094>]**
Description	This command is used to modify a database entry.
Parameters	*mac* – The MAC address that accepts access by local mode. *vlan* – If the MAC address is authorized, the port will be assigned to this VLAN. *vlanid <vlanid 1-4094>* – the vlan id of specified VLAN,the range of the VLAN ID is from 1 to 4094. If the MAC address is authorized, the port will be assigbed to this VLAN.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config MAC-based access control local:

```
DGS-3700-12:5#config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default
Command: config mac_based_access_control_local mac 00-00-00-00-00-01 vlan default

Success.

DGS-3700-12:5#
```

delete mac_based_access_control_local

Purpose	Used to delete the local database entry.
Syntax	**delete mac_based_access_control_local [mac <macaddr> |vlan <vlan_name 32>|vlanid <vlanid 1-4094>]**
Description	This command is used to delete a database entry.
Parameters	*mac* – Delete the database entry by this MAC address. *vlan* – Delete the database entry by this VLAN name. *vlanid <vlanid 1-4094>* – Delete the database entry by this VLAN ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete MAC-based access control local by MAC address:

```
DGS-3700-12:5#delete mac_based_access_control_local mac 00-00-00-00-00-01
Command: delete mac_based_access_control_local mac 00-00-00-00-00-01

Success.

DGS-3700-12:5#
```

To delete MAC-based access control local by VLAN name:

```
DGS-3700-12:5#delete mac_based_access_control_local vlan default
Command: delete mac_based_access_control_local vlan default

Success.

DGS-3700-12:5#
```

To delete mac_based_access_control_local by VLAN ID:

```
DGS-3700-12G:5# delete mac_based_access_control_local vlanid  2
Command: delete mac_based_access_control_local vlanid 2

Success.

DGS-3700-12G:5#
```

show mac_based_access_control

Purpose	Used to display the MAC-based access control setting.
Syntax	**show mac_based_access_control {ports [<portlist> | all]}**
Description	This command is used to display the MAC-based access control setting.
Parameters	*ports* – Display the MAC-based access control port state.
Restrictions	None.

Example usage:

To show MAC-based access control:

```
DGS-3700-12:5#show mac_based_access_control
Command: show mac_based_access_control

MAC Based Access Control
-----------------------------------
State                   : Disabled
Method                  : Local
Password                : default
Guest VLAN              : ----
Guest VLAN VID          : ----
Guest VLAN Member Ports: ----

DGS-3700-12:5#
```

To show MAC-based access control port:

```
DGS-3700-12:5#show mac_based_access_control ports 1-9
Command: show mac_based_access_control ports 1-9

Port    State      Aging Time   Hold Time   Auth Mode
                     (mins)      (secs)
------  --------   ----------   ---------   ----------
1       Disabled   1440         300         Host_based
2       Disabled   1440         300         Host_based
3       Disabled   1440         300         Host_based
4       Disabled   1440         300         Host_based
5       Disabled   1440         300         Host_based
6       Disabled   1440         300         Host_based
7       Disabled   1440         300         Host_based
8       Disabled   1440         300         Host_based
9       Disabled   1440         300         Host_based

DGS-3700-12:5#
```

show mac_based_access_control_local

Purpose	Used to display the MAC-based Access Control local database.
Syntax	**show mac_based_access_control_local {[mac <macaddr>|vlan<vlan_name 32>|vlanid <vlanid 1-4094>]}**
Description	This command is used to display the MAC-based Access Control local database.
Parameters	*mac* – Display the MAC-based access control local database by this MAC address. *vlan<vlan_name 32>* – Display mac_based_access_control local database by this VLAN name. *vlanid <vlanid 1-4094>* – Display mac_based_access_control local database by this VLAN ID.
Restrictions	None.

Example usage:

To show MAC-based access control local:

```
DGS-3700-12:5#show mac_based_access_control_local
Command: show mac_based_access_control_local

MAC Address                   VLAN Name              VID
----------------  -------------------------------  ------
00-00-00-00-00-05             default                 1
00-00-00-00-00-06             VLAN2                   2

Total Entries:2

DGS-3700-12:5#
```

To show MAC-based access control local by MAC address:

```
DGS-3700-12:5#show mac_based_access_control_local mac 00-00-00-00-00-05
Command: show mac_based_access_control_local mac 00-00-00-00-00-05

MAC Address                   VLAN Name              VID
----------------  -------------------------------  ------
00-00-00-00-00-05            default                 1

Total Entries:1

DGS-3700-12:5#
```

To show MAC-based access control local by VLAN name:

```
DGS-3700-12:5#show mac_based_access_control_local vlan VLAN2
Command: show mac_based_access_control_local vlan VLAN2

MAC Address                   VLAN Name              VID
----------------  -------------------------------  ------
00-00-00-00-00-06             VLAN2                   2

Total Entries:1

DGS-3700-12:5#
```

To show mac_based_access_control_local by vlan id:

```
DGS-3700-12:5#show mac_based_access_control_local vlanid 1
Command: show mac_based_access_control_local vlanid 1

MAC Address                  VLAN Name             VID
---------------  -------------------------------  ------
00-00-00-00-00-05              default               1

Total Entries:1

DGS-3700-12:5#
```

show mac_based_access_control auth_mac

Purpose	Used to display MAC-based access control authentication status.
Syntax	**show mac_based_access_control auth_mac {ports <portlist>}**
Description	This command is used to display MAC-based access control authentication status.
Parameters	*ports* – Display authentication status by port.
Restrictions	None.

Example usage:

To show MAC-based access control authentication status:

```
DGS-3700-12:5#show mac_based_access_control auth_mac
Command: show mac_based_access_control auth_mac

Port number : 1
Index    MAC Address         Auth State          VLAN Name   VID
-----  -----------------    --------------       ----------  --------
1      00-00-01-02-03-A2    Authenticated        default     1
2      00-03-09-18-10-01    Authenticated        default     1
3      00-05-5D-ED-84-EA    Authenticated        default     1
4      00-0D-0B-4E-A0-F7    Authenticated        default     1
5      00-0D-60-8F-49-38    Authenticated        default     1
6      00-0E-A6-8E-C1-B7    Authenticated        default     1
7      00-10-4B-69-F4-AD    Authenticated        default     1
8      00-11-D8-DA-CE-0B    Authenticated        default     1
9      00-15-E9-C4-FD-A0    Authenticated        default     1
10     00-54-85-77-00-03    Authenticated        default     1
11     00-80-C8-39-41-DD    Authenticated        default     1
12     00-80-C8-58-72-1B    Authenticated        default     1
13     00-80-C8-DF-E8-02    Authenticated        default     1
14     00-A0-C9-01-01-23    Authenticated        default     1
15     00-E0-18-45-C7-28    Authenticated        default     1
16     00-E0-18-FB-43-3E    Authenticated        default     1

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

clear mac_based_access_control auth_mac

Purpose	Used to reset the current state of a user. The re-authentication will be started after the user traffic is received again.
Syntax	**clear mac_based_access_control auth_mac [ports [all | <portlist>] | mac_addr <macaddr>]**
Description	This command is used to clear the authentication state of a user (or port). The port (or the user) will return to un-authenticated state. All the timer associated with the port (or the user) will be reset.
Parameters	*ports* – To specify the port range to delete MAC on them . *mac_addr* – To delete a specified host with this MAC
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage

To clear the MAC being processed by MAC-Based Access Control.

```
DGS-3700-12:5#clear mac_based_access_control auth_mac ports all
Command: clear mac_based_access_control auth_mac ports all

Success.

DGS-3700-12:5#
```

54

WEB-BASED ACCESS CONTROL COMMANDS

The Web-based Access Control commands in the Command Line Interface (CLI) are listed (along with the appropriate parameters) in the following table.

Command	Parameters
enable wac	
disable wac	
config wac	{ vlan <vlan_name 32> | ports [<portlist> | all] | state [enable | disable] | method [local | radius] | | default_redirpath <string 128> | logout_timer [infinite |<min 1-1440>]}(1)
create wac user	<username 15> vlan <vlan_name 32>
delete wac user	<username 15>
config wac user	<username 15> vlan <vlan_name 32>
show wac	{ports [<portlist> | all]}
show wac user	
clear wac auth_state ports	[<portlist> | all]

Each command is listed, in detail, in the following sections.

enable wac

Purpose	Used to enable the Web-based access control function.
Syntax	**enable wac**
Description	This command is used to enable the WAC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable the WAC function:

```
DGS-3700-12:5#enable wac
Command: enable wac

Success.

DGS-3700-12:5#
```

disable wac

Purpose	Used to disable the Web-based access control function.
Syntax	**disable wac**
Description	This command is used to disable the WAC function.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the WAC function:

```
DGS-3700-12:5#disable wac
Command: disable wac

Success.

DGS-3700-12:5#
```

config wac

Purpose	Used to configure the parameters of the web authentication.
Syntax	**config wac { vlan <vlan_name 32> | ports [<portlist> | all] | state [enable | disable] | method [local | radius] | default_redirpath <string 128> | logout_timer [infinite | <min 1-1440>]}(1)**
Description	This command is used to configure Web-based-function setting. The specific VLAN which assigned to authentication vlan must be existed already.
Parameters	*ports* – A range of ports used to enable or disable wac function. *state* – Specify specific port state. *method* – Specify which authenticated method *vlan* – Authentication vlan name. *default_redirpath* – The URL that the client will be redirected to after successful authentication. Initially, the redirected path is empty string. It must be specified by the user before the function can be enabled. *logout_timer* – The authenticated port will be reverted to un-authenticated state after logout timer. The default value is *60* minutes. "infinite" indicates that the authentiucated port never ages out.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port state:

```
DGS-3700-12:5#config wac ports 1-8 state enable
Command: config wac ports 1-8 state enable

Success.

DGS-3700-12:5#
```

To configure the method RADIUS:

```
DGS-3700-12:5#config wac method radius
Command: config wac method radius

Success.

DGS-3700-12:5#
```

To configure authentication VLAN:

```
DGS-3700-12:5#config wac vlan default
Command: config wac vlan default

Success.

DGS-3700-12:5#
```

create wac user

Purpose	Used to create user account for web-based access control .
Syntax	**create wac user <username 15> vlan <vlan_name 32>**
Description	This command is used to create account for web-base access control. This user account is independent with login user acoount.
Parameters	*username* – User account for web-base access control. *vlan* – Authentication vlan name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a WAC account:

```
DGS-3700-12:5#create wac user 123 vlan default
Command: create wac user 123 vlan default

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

DGS-3700-12:5#
```

delete wac user

Purpose	Used to delete the account for Web-based access control.
Syntax	**delete wac user <username 15>**
Description	This command is used to delete an account.
Parameters	*username* – User account for Web-based access control.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a WAC account:

```
DGS-3700-12:5#delete wac user 123
Command: delete wac user 123

Success.

DGS-3700-12:5#
```

config wac user

Purpose	Used to configure the VLAN ID of the user account.
Syntax	**config wac user <username 15> vlan <vlan_name 32>**
Description	This command is used to configure Web-based-function user setting.
Parameters	*username* – The name of the user account to be changed. *vlan* – Authentication VLAN name.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the port state:

```
DGS-3700-12:5#config wac user 123 vlan default
Command: config wac user 123 vlan default

Success.

DGS-3700-12:5#
```

show wac

Purpose	Used to displayWweb authentication settings.
Syntax	**show wac {ports [<portlist>| all]}**
Description	This command is used to display the Web authentication setting.
Parameters	*ports* – A range of member ports to show the status. *all* – Will show the status of all the member ports.
Restrictions	None.

Example usage:

To display the WAC state:

```
DGS-3700-12:5#show wac
Command: show wac

Web Based Access Control
----------------------------
State               : Enable
Method              : RADIUS
VLAN                : default
Logout Timer        : 60 mins
Redirection Page    : http://tw.yaholl.com


DGS-3700-12:5#
```

To display WAC ports:

```
DGS-3700-12:5#show wac ports 1-8
Command: show wac ports 1-8

Port        State        User Name     Auth State       Assigned Vlan
----       -------       ----------   ------------    ---------------
1           Enabled        123         Authenticated         12
2           Enabled        abc         Authenticating         -
3           Enabled        Apple       Un-authenticated       -
4           Enabled         -              -                   -
5           Enabled         -              -                   -
6           Enabled         -              -                   -
7           Enabled         -              -                   -
8           Enabled         -              -                   -

DGS-3700-12:5#
```

show wac user

Purpose	Used to display the user account for web authentication.
Syntax	**show wac user**
Description	This command is used to show web authentication account.
Parameters	None.
Restrictions	None.

Example usage:

To show Web authentication account:

```
DGS-3700-12:5#show wac user
Command: show wac user

Current Accounts:
Username           Vlan Name
---------------    ---------
123                default

Total Entries: 1

DGS-3700-12:5#
```

clear wac auth_state

Purpose	Used to clear the authentication state of a port.
Syntax	**clear wac auth_state ports [<portlist> |all]**
Description	This command is used to clear the authentication state of a port. The port will return to an un-authenticated state. All the timers associated with the port will be reset.
Parameters	*<portlist>* – Specifies the list of ports whose WAC state will be cleared. *all* – Specifies all the ports whose WAC state will be cleared.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the WAC authenticated state:

```
DGS-3700-12:5#clear wac auth_state ports 1-5
Command: clear wac auth_state ports 1-5

Success.

DGS-3700-12:5#
```

55

FILTER COMMANDS (DHCP SERVER/NETBIOS)

DHCP Server Screening Settings

This function allows you not only to restrict all DHCP Server packets but also to receive any specified DHCP server packets by any specified DHCP client, it is useful when one or more than one DHCP servers are present on the network and both provide DHCP services to different distinct groups of clients. Enabling the DHCP filter for the first time will create both an access profile and access rule per port, following this other access rules can be created. These rules are used to block all DHCP server packets. Similarly, the addition of a permit DHCP entry will create one access profile and one access rule the first time the DHCP client MAC address is the client MAC address, and the Source IP address is the same as the DHCP server's IP address (UDP port number 67). These rules are used to permit the DHCP server packets with specific fileds, which the user configures.

When the DHCP Server filter function is enabled, all DHCP Server packets will be filtered from a specific port. Also, you are allowed to create entries for specific port-based Server IP address and Client MAC address binding entries. Be aware that the DHCP Server filter function must be enabled first. Once all settings are complete, all DHCP Server packets will be filtered from a specific port except those that meet the Server IP Address and Client MAC Address binding.

NetBIOS Filtering Setting

When the NetBIOS filter is enabled, all NetBIOS packets will be filtered from the specified port. Enabling the NetBIOS filter will create one access profile and create three access rules per port (UDP port numbers 137 and 138 and TCP port number 139).

For Extensive NetBIOS Filter, when it is enabled, all NetBIOS packets over 802.3 frames will be filtered from the specified port. This command is used to configure the state of the NetBIOS filter. Enabling the Extensive NetBIOS filter will create one access profile and create one access rule per port (DSAP (Destination Service Access Point) =F0, and SASP (Source Service Access Point) =F0).

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

Command	Parameters
config filter dhcp_server	[add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>| all] |delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all]|ports [<portlist> | all] state [enable | disable]]
show filter dhcp_server	
config filter netbios	[<portlist> | all] state [enable|disable]
show filter netbios	
config filter extensive_netbios	[<portlist> | all] state [enable|disable]
show filter extensive_netbios	

Each command is listed, in detail, in the following sections.

config filter dhcp_server

Purpose	DHCP server packets except those that have been IP/client MAC bound will be filtered. This command is used to configure the state of the function for filtering of DHCP server packet and to add/delete the DHCP server/client binding entry.
Syntax	**config filter dhcp_server [add permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all] |delete permit server_ip <ipaddr> {client_mac <macaddr>} ports [<portlist>|all]|ports [<portlist> | all] state [enable | disable]]**
Description	This command has two purposes: to filter all DHCP server packets on the specified port(s) and to allow some DHCP server packets to be forwarded if they are on the pre-defined server IP address/MAC address binding list. Thus the DHCP server can be restricted to service a specified DHCP client. This is useful when there are two or more DHCP servers present on a network.
Parameters	*ippaddr* – The IP address of the DHCP server to be filtered *macaddr* – The MAC address of the DHCP client. *state* – Enable/Disable the DHCP filter state *ports <portlist>* – The port number to which the DHCP filter will be applied.
Restrictions	Only Administrator-level users can issue this command. Enabling the DHCP filter will create one access profile and create one access rule per port (UDP port 67). Addition of a DHCP filter permit entry will create one access profile and create one access rule (DA = client MAC address, SA = source IP address and UDP port 67).

Example usage:

To add an entry from the DHCP server/client filter list in the switch's database:

```
DGS-3700-12:5#config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-
00-00-00-00-01 port 1-12
Command: config filter dhcp_server add permit server_ip 10.1.1.1 client_mac 00-00-00-
00-00-01 port 1-12

Success

DGS-3700-12:5#
```

To configure the DHCP filter state:

```
DGS-3700-12:5#config filter dhcp_server ports 1-10 state enable
Command: config filter dhcp_server ports 1-10 state enable

Success

DGS-3700-12:5#
```

show filter dhcp_server

Purpose	Used to display current DHCP server/client filter list created on the switch.
Syntax	**show filter dhcp_server**
Description	This command is used to display DHCP server/client filter list created on the switch.
Parameters	None.
Restrictions	Only Administrator users can issue this command.

Example usage:

To display the DHCP server filter list created on the switch:

```
DGS-3700-12:5#show filter dhcp_server
Command: show filter dhcp_server

Enabled Ports: 1-3

Filter DHCP Server/Client Table
Server IP Address   Client MAC Address   Port
-----------------   ------------------   -------------
10.255.255.254      00-00-00-00-00-01    1-12

 Total Entries: 1

DGS-3700-12:5#
```

config filter netbios

Purpose	Used to configure the switch to filter NetBIOS packets from specified ports.
Syntax	**config filter netbios [<portlist> | all] state [enable|disable]**
Description	This command will configure the switch to filter NetBIOS packets from the specified ports.
Parameters	*[<portlist>|all]* – The list of port numbers to which the NetBIOS filter will be applied. *state [enable|disable]* – Used to enable/disable the NetBIOS filter on the switch.
Restrictions	Only Administrator-level users can issue this command. Enabling the NetBIOS filter will create one access profile and three access rules per port (UDP port number 137 and 138, and TCP port 139).

Example usage:

To configure the NetBIOS state:

```
DGS-3700-12:5#config filter netbios 1-10 state enable
Command: config filter netbios 1-10 state enable

Success.

DGS-3700-12:5#
```

show filter netbios

Purpose	Used to display the switch settings to filter NetBIOS packets from specified ports.
Syntax	**show filter netbios**
Description	This command will display the switch settings to filter NetBIOS packets from the specified ports.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the extensive NetBIOS filter status:

```
DGS-3700-12:5#show filter netbios
Command: show filter netbios

Enabled Ports: 1-3

DGS-3700-12:5#
```

config filter extensive_netbios

Purpose	Used to configure the switch to filter 802.3 frame NetBIOS packets from specified ports.
Syntax	**config filter extensive_netbios [<portlist>|all] state [enable|disable]**
Description	This command will configure the switch to filter 802.3 frame NetBIOS packets from the specified ports.
Parameters	*[<portlist>|all]* – The list of port numbers to which the NetBIOS filter will be applied. *state [enable|disable]* – Used to enable/disable the NetBIOS filter on the switch.
Restrictions	Only Administrator-level users can issue this command. Enabling the NetBIOS filter will create one access profile and one access rules per port (DSAP=F0, SASP=F0).

Example usage:

To configure the extensive NetBIOS state::

```
DGS-3700-12:5#config filter extensive_netbios 1-10 state enable
Command: config filter extensive_netbios 1-10 state enable

Success.

DGS-3700-12:5#
```

show filter extensive_netbios

Purpose	Used to display the switch settings to filter NetBIOS packets from specified ports.
Syntax	**show filter extensive_netbios**
Description	This command will display the switch settings to filter NetBIOS packets from the specified ports.
Parameters	None.
Restrictions	Only Administrator-level users can issue this command.

Example usage:

To display the extensive NetBIOS filter status:

```
DGS-3700-12:5#show filter extensive_netbios
Command: show filter extensive_netbios

Enabled Ports: 1-3

DGS-3700-12:5#
```

56

ACCESS CONTROL LIST (ACL) COMMANDS

The Switch implements Access Control Lists that enable the Switch to deny network access to specific devices or device groups based on IP settings and MAC address.

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

Note: The ACL command set has been changed for the Release III firmware. In particular, note the different role of the *profile_id* and *access_id* parameters. The new treatment has changed some of the command parameters as well.

Command	Parameters
create access_profile	<value 1-12> profile_name <name 1-32>[ethernet{ vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}(1) | ip { vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}(1) | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}(1) | packet_content_mask { offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1) | ipv6 {[{ class | flowlabel |[tcp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>}]}(1) | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]}(1)
delete access_profile	[profile_id <value 1-12> | all | profile_name <name 1-32 >]
config access_profile	[profile_id <value 1-12> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-128>][ethernet {[vlan <vlan_name 32>|vlan_id <value 1-4094>]|source_mac <macaddr 000000000000-ffffffffffff>|destination_mac <macaddr 000000000000-ffffffffffff>|802.1p <value 0-7>|ethernet_type <hex 0x0-0xffff>}(1) | ip{[vlan <vlan_name 32>|vlan_id <value 1-4094>]|source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp {type <value 0-255>|code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>|urg|ack|psh|rst|syn|fin}(1)|udp {src_port <value 0-65535>|dst_port <value 0-65535>}|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}(1) | packet_content { offset_chunk_1 <hex 0x0-0xffffffff>| offset_chunk_2 <hex 0x0-0xffffffff>| offset_chunk_3 <hex 0x0-0xffffffff>| offset_chunk_4 <hex 0x0-0xffffffff>}(1) | ipv6 {[{ class <value 0-255>| flowlabel <hex 0x0-0xfffff> |[tcp { src_port <value 0-65535> | dst_port <value 0-65535> } | udp { src_port <value 0-65535> | dst_port <value 0-65535>}]}(1) | source_ipv6 <ipv6addr>| destination_ipv6 <ipv6addr>]}(1)] [port [<portlist>|all] | vlanbased [vlan <vlan_name> | vlan_id <value 1-4094>]] [permit {priority <value 0-7> {replace_priority} |rx_rate [no_limit|<value 1-15624>]|[replace_dscp_with <value 0-63>|replace_tos_precedence_with <value 0-7>]|counter[enable|disable]} |mirror |deny] {time_range <range_name 32>}|delete access_id <value 1-128>]
show access_profile	{profile_id <value 1-12>| profile_name <name 1-32 >}
enable cpu_interface_filtering	
disable cpu_interface_filtering	
create cpu access_profile profile_id	<value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff > | destination_mac <macmask 000000000000-ffffffffffff > | 802.1p | ethernet_type}(1) | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> |

Command	Parameters
	dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}(1)]} | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask {<hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}(1) | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>| offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}(1) | ipv6 { class | flowlabel | }(1) | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]}(1)]
delete cpu access_profile	[profile_id <value 1-5 | all]
config cpu access_profile	profile_id <value 1-5>[add access_id <value 1-100>[ethernet {vlan <vlan_name 32>|vlan_id <value 1-4094>] | source_mac <macaddr 000000000000-ffffffffffff>|destination_mac <macaddr 000000000000-ffffffffffff>|802.1p <value 0-7> |ethernet_type <hex 0x0-0xffff>}(1) | ip{[vlan <vlan_name 32> | vlan_id <value 1-4094>] |source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp{type <value 0-255>|code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>|urg|ack|psh|rst|syn|fin}(1)|udp {src_port <value 0-65535>|dst_port <value 0-65535>}|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}(1) | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}(1) | ipv6 {[{ class <value0-255>| flowlabel <hex 0x0-0xfffff>}(1)| source_ipv6 <ipv6addr>| destination_ipv6 <ipv6addr>]}(1)] port [<portlist> | all][permit | deny] {time_range <range_name 32>}| delete access_id <value 1-100>]
show cpu access_profile	profile_id <value 1-5>
config flow_meter	[profile_id <value 1-12> | profile_name <name 1-32>] access_id <value 1-128>[[tr_tcm cir <value 0-15624> {cbs <value 0-16384>} pir <value 0-15624> {pbs <value 0-16384>}|sr_tcm cir <value 0-15624> cbs <value 0-16384> ebs <value 0-16384>] {conform permit {replace_dscp <value 0-63>} {counter [enable |disable]}} exceed [permit {replace_dscp <value 0-63>} {counter [enable |disable]} | drop] violate [permit {replace_dscp <value 0-63>} {counter [enable |disable]} | drop] |delete]
show flow_meter	{ [profile_id < value 1-12> | profile_name <name 1-32>] { access_id < value 1-128 >}}
config time_range	<range_name 32> [hours start_time < time hh:mm:ss > end_time< time hh:mm:ss > weekdays <daylist> | delete]
show time_range	
show current_config access_profile	

Access profiles allow users to establish criteria to determine whether or not the Switch will forward packets based on the information contained in each packet's header.

Creating an access profile is divided into two basic parts. First, an access profile must be created using the **create access_profile** command. For example, if users want to deny all traffic to the subnet 10.42.73.0 to 10.42.73.255, users must first **create** an access profile that instructs the Switch to examine all of the relevant fields of each frame.

First create an access profile that uses IP addresses as the criteria for examination:

create access_profile profile_id 1 profile_name 1 ip source_ip_mask 255.255.255.0

Here we have created an access profile that will examine the IP field of each frame received by the Switch. Each source IP address the Switch finds will be combined with the **source_ip_mask** with a logical AND operation. The **profile_id** parameter is used to give the access profile an identifying number – in this case, 1 – and it is used to assign a priority in case a conflict occurs. The

profile_id establishes a priority within the list of profiles. A lower **profile_id** gives the rule a higher priority. In case of a conflict in the rules entered for different profiles, the rule with the highest priority (lowest profile_id) will take precedence. *See below for information regarding limitations on access profiles and access rules.*

The **deny** parameter instructs the Switch to filter any frames that meet the criteria – in this case, when a logical AND operation between an IP address specified in the next step and the **ip_source_mask** match.

The default for an access profile on the Switch is to **permit** traffic flow. If users want to restrict traffic, users must use the **deny** parameter.

Now that an access profile has been created, users must add the criteria the Switch will use to decide if a given frame should be forwarded or filtered. We will use the **config access_profile** command to create a new rule that defines the criteria we want. Let's further specify in the new rule to deny access to a range of IP addresses through an individual port: Here, we want to filter any packets that have an IP source address between 10.42.73.0 and 10.42.73.255, and specify the port that will not be allowed:

config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1 port 7 deny

We use the **profile_id 1** which was specified when the access profile was created. The **add** parameter instructs the Switch to add the criteria that follows to the list of rules that are associated with access profile 1. For each rule entered into the access profile, users can assign an access_id that identifies the rule within the list of rules. The access_id is an index number and does not effect priority within the **profile_id**. This access_id may be used later if users want to remove the individual rule from the profile.

The **ip** parameter instructs the Switch that this new rule will be applied to the IP addresses contained within each frame's header. **source_ip** tells the Switch that this rule will apply to the source IP addresses in each frame's header. The IP address **10.42.73.1** will be combined with the **source_ip_mask 255.255.255.0** to give the IP address 10.42.73.0 for any source IP address between 10.42.73.0 to 10.42.73.255. Finally the restricted port - port number 7 - is specified.

Due to a chipset limitation, the Switch supports a maximum of twelve access profiles. The rules used to define the access profiles are limited to a total of 1536 rules for the Switch.

create access_profile

Purpose	Used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **create access_profile** command, below.
Syntax	**create access_profile profile_id <value 1-12> profile_name <name 1-32> [ethernet{ vlan | source_mac <macmask 000000000000-ffffffffffff> | destination_mac <macmask 000000000000-ffffffffffff> | 802.1p | ethernet_type}(1) |ip { vlan| source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code } | igmp {type } | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> | flag_mask [all | {urg | ack | psh | rst | syn | fin}(1) | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xff> {user_define_mask <hex 0x0-0xffffffff>}]}(1) | packet_content_mask { offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff> | offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff>}(1)|ipv6 {[{ class | flowlabel |[tcp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | udp { src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff> }]}(1) | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]}(1)**
Description	This command is used to create an access profile on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Parameters	*profile_id <value 1-12>* – Sets the relative priority for the profile. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 - 12, yet, remember only 12 access profiles can be created on the Switch. *profile_name <name 1-32>* – Specifies the name of the profile. The maximum length is 32 characters. *ethernet* – Specifies that the Switch will examine the layer 2 part of each packet header. • *vlan* – Specifies that the Switch will examine the VLAN part of each packet header. source_mac <macmask 000000000000-ffffffffffff > – Specifies a MAC address mask

create access_profile

for the source MAC address. This mask is entered in a hexadecimal format.

- *destination_mac <macmask 000000000000-ffffffffffff >* – Specifies a MAC address mask for the destination MAC address.
- *802.1p* – Specifies that the Switch will examine the 802.1p priority value in the frame's header.
- *ethernet_type* – Specifies that the Switch will examine the Ethernet type value in each frame's header.

ip – Specifies that the Switch will examine the IP address in each frame's header.

vlan – Specifies a VLAN mask.

source_ip_mask <netmask> – Specifies an IP address mask for the source IP address.

destination_ip_mask <netmask> – Specifies an IP address mask for the destination IP address.

dscp – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.

icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.

- *type* – Specifies that the Switch will examine each frame's ICMP Type field.
- *code* – Specifies that the Switch will examine each frame's ICMP Code field.

igmp – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.

type – Specifies that the Switch will examine each frame's IGMP Type field.

tcp – Specifies that the Switch will examine each frame's Transmission Control Protocol (TCP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a TCP port mask for the destination port.

flag_mask – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between *all, urg* (urgent), *ack* (acknowledgement), *psh* (push), *rst* (reset), *syn* (synchronize) and *fin* (finish).

udp – Specifies that the Switch will examine each frame's User Datagram Protocol (UDP) field.

src_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the source port.

dst_port_mask <hex 0x0-0xffff> – Specifies a UDP port mask for the destination port.

protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

user_define_mask <hex 0x0-0xffffffff> – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

packet_content_mask – Allows users to examine up to 4 specified offset_chunk within a packet at one time and specifies that the Switch will mask the packet header beginning with the offset value specified as follows:

packet_content_mask {offset_chunk_1 <value 0-31> <hex 0x0-0xffffffff>| offset_chunk_2 <value 0-31> <hex 0x0-0xffffffff>| offset_chunk_3 <value 0-31> <hex 0x0-0xffffffff>|offset_chunk_4 <value 0-31> <hex 0x0-0xffffffff> }

With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link switches can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is the reason why Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

IPV6 – Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the **config access_profile** command for IPv6.

create access_profile

	• *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4. • *flowlabel* – Entering this parameter will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets. • *tcp* – Specifies that the Switch will examine each frame's Transmission Control Protocol (TCP) field. • *udp* – Specifies that the Switch will examine each frame's User Datagram Protocol (UDP) field. • *source_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the source IPv6 address. • *destination_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the destination IPv6 address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create an access list rules:

```
DGS-3700-12:5#create access_profile profile_id 5 profile_name 5 ethernet vlan
source_mac 00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type
Command: create access_profile profile_id 5 profile_name 5 ethernet vlan source_mac
00-00-00-00-00-01 destination_mac 00-00-00-00-00-02 802.1p ethernet_type

Success.

DGS-3700-12:5#
```

delete access_profile

Purpose	Used to delete a previously created access profile.
Syntax	**delete access_profile [profile_id <value 1-12> | all | profile_name <name 1-32 >]**
Description	This command is used to delete a previously created access profile on the Switch.
Parameters	*profile_id <value 1-12>* – Enter an integer between 1 and 12 that is used to identify the access profile that will be deleted with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The user may enter a profile ID number between 1 and 12, yet, remember only 12 access profiles can be created on the Switch. *profile_name <name 1-32>* – Specifies the name of the profile. The maximum length is 32 characters. *all* – Entering this parameter will delete all access profiles currently configured on the Switch.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the access profile with a profile ID of 1:

```
DGS-3700-12:5#delete access_profile profile_id 1
Command: delete access_profile profile_id 1

Success.

DGS-3700-12:5#
```

config access_profile

Purpose	Used to configure an access profile on the Switch and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the **create access_profile** command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config access_profile** command, below.
Syntax	**[profile_id <value 1-12> | profile_name <name 1-32>] [add access_id [auto_assign | <value 1-128>][ethernet {[vlan <vlan_name 32>|vlan_id <value 1-4094>]|source_mac <macaddr 000000000000-ffffffffffff>|destination_mac <macaddr 000000000000-ffffffffffff>|802.1p <value 0-7>|ethernet_type <hex 0x0-0xffff>}|ip{[vlan <vlan_name 32>|vlan_id <value 1-4094>]|source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp {type <value 0-255>|code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>|urg|ack|psh|rst|syn|fin}(1)|udp {src_port <value 0-65535>|dst_port <value 0-65535>}|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}|packet_content { offset_chunk_1 <hex 0x0-0xffffffff>| offset_chunk_2 <hex 0x0-0xffffffff>| offset_chunk_3 <hex 0x0-0xffffffff>| offset_chunk_4 <hex 0x0-0xffffffff>}|ipv6 {[{ class <value 0-255>| flowlabel <hex 0x0-0xfffff> |[tcp { src_port <value 0-65535> | dst_port <value 0-65535> } | udp { src_port <value 0-65535> | dst_port <value 0-65535> }]}| source_ipv6 <ipv6addr>| destination_ipv6 <ipv6addr>]}] [port [<portlist>|all] | vlanbased [vlan <vlan_name> | vlan_id <value 1-4094>]] [permit {priority <value 0-7> {replace_priority} |rx_rate [no_limit|<value 1-15624>]|[replace_dscp_with <value 0-63>|replace_tos_precedence_with <value 0-7>]|counter[enable|disable]} |mirror |deny] {time_range <range_name 32>}|delete access_id <value 1-128>]**
Description	This command is used to configure an access profile on the Switch and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **create access_profile** command, above.
Parameters	*profile_id <value 1-12>* – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 and 12, yet, remember only 12 access profiles can be created on the Switch. *profile_name<name 1-32>* – Specifies the name of the profile. The maximum length is 32 characters. *add access_id <value 1-128>* – Adds an additional rule to the above specified access profile. The value is used to index the rule created. For information on number of rules that can be created for a given port, lease see the introduction to this chapter. *ethernet* – Specifies that the Switch will look only into the layer 2 part of each packet. *vlan <vlan_name 32>|vlan_id <value 1-4094>* – Specifies that the access profile will apply to only to this VLAN. *source_mac <macaddr 000000000000-ffffffffffff >* – Specifies that the access profile will apply to only packets with this source MAC address. *destination_mac <macaddr 000000000000-ffffffffffff >* – Specifies that the access profile will apply to only packets with this destination MAC address. *802.1p <value 0-7>* – Specifies that the access profile will apply only to packets with this 802.1p priority value. *ethernet_type <hex 0x0-0xffff>* – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.
Parameters	*ip* – Specifies that the Switch will look into the IP fields in each packet. *vlan <vlan_name 32>|vlan_id<value 1-4094>* – Specifies that the access profile will apply to only this VLAN. *source_ip <ipaddr>* – Specifies that the access profile will apply to only packets with this source IP address.

config access_profile

destination_ip <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.

dscp <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header

icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

type <value 0-65535> – Specifies that the access profile will apply to this ICMP type value.

code <value 0-255> – Specifies that the access profile will apply to this ICMP code.

igmp – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

type <value 0-255> – Specifies that the access profile will apply to packets that have

this IGMP type value.

tcp – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.

- *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
- *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.

urg: TCP control flag (urgent)

ack: TCP control flag (acknowledgement)

psh: TCP control flag (push)

rst: TCP control flag (reset)

syn: TCP control flag (synchronize)

fin: TCP control flag (finish)

udp – Specifies that the Switch will examine the User Datagram Protocol (UDP) field in each packet.

src_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP source port in their UDP header.

dst_port <value 0-65535> – Specifies that the access profile will apply only to packets that have this UDP destination port in their UDP header.

protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

user_define <hex 0x0-0xffffff> – Specifies a mask to be combined with the value found in the frame header and if this field contains the value entered here, apply the following rules.

packet_content_mask – Allows users to examine any up to four specified offset_chunk within a packet at one time and specifies that the Switch will mask the packet header beginning with the offset value specified as follows:

packet_content { offset_chunk_1 <hex 0x0-0xffffffff>| offset_chunk_2 <hex 0x0-0xffffffff>| offset_chunk_3 <hex 0x0-0xffffffff>| offset_chunk_4 <hex 0x0-0xffffffff>

With this advanced unique Packet Content Mask (also known as Packet Content Access Control List - ACL), D-Link switches can effectively mitigate some network attacks like the common ARP Spoofing attack that is wide spread today. This is the reason that Packet Content ACL is able to inspect any specified content of a packet in different protocol layers.

IPV6 - Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the **config access_profile** command for IPv6.

- *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4.
- *flowlabel* – Entering this parameter will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets.

config access_profile

	• *tcp* – Specifies that the Switch will examine each frame's Transmission Control Protocol (TCP) field. • *udp* - Specifies that the Switch will examine each frame's User Datagram Protocol (UDP) field. • *source_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the source IPv6 address. • *destination_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the destination IPv6 address.
Parameters	*port <portlist>* – Specifies the port number on the Switch to permit or deny access for the rule. *vlanbased [vlan <vlan_name> | vlan_id <value 1-4094>]* – Specifies that the access profile will apply to only to this VLAN. *permit* – Specifies the rule permit access for incoming packets on the previously specified port. *priority <value 0-7>* – Specifies that the access profile will apply to packets that contain this value in their 802.1p priority field of their header for incoming packets on the previously specified port. *{replace_priority}* – Allows users to specify a new value to be written to the priority field of an incoming packet on the previously specified port. *replace_dscp_with <value 0-63>* – Allows users to specify a new value to be written to the DSCP field of an incoming packet on the previously specified port. *replace_tos_precedence_with <value 0-7>* – Specifies the packets that match the access profile and that tos-precedence values will be changed by the switch. *rx_rate* – Specifies that one of the parameters below (*no_limit* or *<value 1-15624>*) will be applied to the rate at which the above specified ports will be allowed to receive packets • *no_limit* – Specifies that there will be no limit on the rate of packets received by the above specified ports. • *<value 1-15624>* – Specifies the packet limit, in 64Kbps, that the above ports will be allowed to receive. *deny* – Specifies the rule will deny access for incoming packets on the previously specified port. *mirror* – Specifies the packets that match the access profile, copies it and sends the copied one to the mirror port. *time_range* – Specifies the time_range profile that has been associated with the ACL entries. *delete access_id <value 1-128>* – Use this to remove a previously created access rule of a profile ID. For information on number of rules that can be created for a given port, lease see the introduction to this chapter.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the access profile with the profile ID of 1 to filter frames on port 7 that have IP addresses in the range between 10.42.73.0 to 10.42.73.255:

```
DGS-3700-12:5#config access_profile profile_id 1 add access_id 1 ip source_ip
10.42.73.1 port 7 deny
Command: config access_profile profile_id 1 add access_id 1 ip source_ip 10.42.73.1
port 7 deny

Success.

DGS-3700-12:5#
```

NOTE: Address Resolution Protocol (ARP) is the standard for finding a host's hardware address (MAC Address). However, ARP is vulnerable as it can be easily spoofed and utilized to attack a LAN (known as ARP spoofing attack). For a more detailed explaination on how ARP protocol works and how to employ D-Link's advanced unique Packet Content ACL to prevent an ARP spoofing attack, please see Appendix B, at the end of this manual.

show access_profile

Purpose	Used to display the currently configured access profiles on the Switch.
Syntax	**show access_profile {profile_id <value 1-12>| profile_name <name 1-32 >}**
Description	This command is used to display the currently configured access profiles.
Parameters	*profile_id <value 1-12>* – Specify the profile id to display only the access rules configuration for a single profile ID. The user may enter a profile ID number between 1 and 12, yet, remember only 12 access profiles can be created on the Switch *profile_name <name 1-32>* – Specifies the name of the profile. The maximum length is 32 characters.
Restrictions	None.

Example usage:

To display all of the currently configured access profiles on the Switch:

```
DGS-3700-12:5#show access_profile
Command: show access_profile

Access Profile Table

Total Unused Rule Entries:1536
Total Used Rule Entries  :0


Access Profile ID: 5                                    Type : Ethernet
================================================================================
Profile Name:5
Owner       : ACL
MASK Option :
VLAN         Source MAC         Destination MAC   802.1P  Ethernet Type
             00-00-00-00-00-01  00-00-00-00-00-02
-----------  -----------------  ----------------- ------  ------------
================================================================================
Unused Entries: 128


DGS-3700-12:5#
```

create cpu access_profile

Purpose	Used to create an access profile specifically for **CPU Interface Filtering** on the Switch and to define which parts of each incoming frame's header the Switch will examine. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **create cpu access_profile** command, below.
Syntax	**create cpu access_profile profile_id <value 1-5> [ethernet {vlan | source_mac <macmask 000000000000-ffffffffffff > | destination_mac <macmask 000000000000-ffffffffffff > | 802.1p | ethernet_type}(1) | ip {vlan | source_ip_mask <netmask> | destination_ip_mask <netmask> | dscp | [icmp {type | code} | igmp {type} | tcp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | flag_mask [all | {urg | ack | psh | rst | syn | fin}(1) | udp {src_port_mask <hex 0x0-0xffff> | dst_port_mask <hex 0x0-0xffff>} | protocol_id_mask <hex 0x0-0xffffffff>} {user_define_mask <hex 0x0-0xffffffff>}](1) | packet_content_mask {offset 0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset 16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | {offset 64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}(1) | ipv6 {[{class | flowlabel|}(1) } | source_ipv6_mask <ipv6mask> | destination_ipv6_mask <ipv6mask>]}(1)]**
Description	This command is used to create an access profile used only for CPU Interface Filtering. Masks can be entered that will be combined with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **create cpu access_profile** command, below.

Parameters	*profile_id <value 1-5>* – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be created with this command.
	ethernet – Specifies that the Switch will examine the layer 2 part of each packet header.
	• *vlan* – Specifies that the Switch will examine the VLAN part of each packet header.
	• *source_mac <macmask 000000000000-ffffffffffff >* – Specifies to examine the source MAC address mask.
	• *destination_mac <macmask 000000000000-ffffffffffff >* – Specifies to examine the destination MAC address mask.
	• *802.1p* – Specifies that the Switch will examine the 802.1p priority value in the frame's header.
	• *ethernet_type* – Specifies that the Switch will examine the Ethernet type value in each frame's header.
	ip – Specifies that the switch will examine the IP address in each frame's header.
	• *vlan* – Specifies a VLAN mask.
	• *source_ip_mask <netmask>* – Specifies an IP address mask for the source IP address.
	• *destination_ip_mask <netmask>* – Specifies an IP address mask for the destination IP address.
	• *dscp* – Specifies that the Switch will examine the DiffServ Code Point (DSCP) field in each frame's header.
	• *icmp* – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field in each frame's header.
	  • *type* – Specifies that the Switch will examine each frame's ICMP Type field.
	  • *code* – Specifies that the Switch will examine each frame's ICMP Code field.
	• *igmp* – Specifies that the Switch will examine each frame's Internet Group Management Protocol (IGMP) field.
	  • *type* – Specifies that the Switch will examine each frame's IGMP Type field.
	• *tcp* – Specifies that the Switch will examine each frames Transmission Control Protocol (TCP) field.
	  • *src_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the source port.
	  • *dst_port_mask <hex 0x0-0xffff>* – Specifies a TCP port mask for the destination port.
	• *flag_mask [all | {urg | ack | psh | rst | syn | fin}]* – Enter the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the

create cpu access_profile

	forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between **all**, **urg** (urgent), **ack** (acknowledgement), **psh** (push), **rst** (reset), **syn** (synchronize) and **fin** (finish). • *udp* – Specifies that the switch will examine each frame's User Datagram Protocol (UDP) field. • *src_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the source port. • *dst_port_mask <hex 0x0-0xffff>* – Specifies a UDP port mask for the destination port. • *protocol_id_mask <hex 0x0-0xffffffff>* – Specifies that the Switch will examine each frame's Protocol ID field using the hex form entered here. • *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header. • *packet_content_mask* – Specifies that the Switch will mask the packet header beginning with the offset value specified as follows: • *offset_0-15* – Enter a value in hex form to mask the packet from byte 0 to byte 15. • *offset_16-31* – Enter a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32-47* – Enter a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* – Enter a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* – Enter a value in hex form to mask the packet from byte 64 to byte 79. *IPV6* – Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the **config access_profile** command for IPv6. • *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4. • *flowlabel* – Entering this parameter will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets. • *source_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the source IPv6 address. *destination_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the destination IPv6 address.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To create a CPU access profile:

```
DGS-3700-12:5#create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code
Command: create cpu access_profile profile_id 1 ip vlan source_ip_mask 20.0.0.0
destination_ip_mask 10.0.0.0 dscp icmp type code

Success.

DGS-3700-12:5#
```

delete cpu access_profile

Purpose	Used to delete a previously created CPU access profile.
Syntax	**delete cpu access_profile [profile_id <value 1-5 | all]**
Description	This command is used to delete a previously created CPU access profile.
Parameters	*profile_id <value 1-5>* – Enter an integer between 1 and 5 that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command. *all* – This will delete all previously configured cpu access_profiles.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete the CPU access profile with a profile ID of 1:

```
DGS-3700-12:5#delete cpu access_profile profile_id 1
Command: delete cpu access_profile profile_id 1

Success.

DGS-3700-12:5#
```

config cpu access_profile

Purpose	Used to configure a CPU access profile used for CPU Interface Filtering and to define specific values that will be used to by the Switch to determine if a given packet should be forwarded or filtered. Masks entered using the **create cpu access_profile** command will be combined, using a logical AND operational method, with the values the Switch finds in the specified frame header fields. Specific values for the rules are entered using the **config cpu access_profile** command, below.
Syntax	**profile_id <value 1-5>[add access_id <value 1-100>[ethernet {[vlan <vlan_name 32>| vlan_id <value 1-4094>] |source_mac <macaddr 000000000000-ffffffffffff>|destination_mac <macaddr 00000000000-ffffffffffff>|802.1p <value 0-7> |ethernet_type <hex 0x0-0xffff>}(1) | ip{[vlan <vlan_name 32>| vlan_id <value 1-4094>] |source_ip <ipaddr>|destination_ip <ipaddr>|dscp <value 0-63>|[icmp{type <value 0-255>|code <value 0-255>}|igmp {type <value 0-255>}|tcp {src_port <value 0-65535>|dst_port <value 0-65535>|urg|ack|psh|rst|syn|fin}(1)|udp {src_port <value 0-65535>|dst_port <value 0-65535>}|protocol_id <value 0-255> {user_define <hex 0x0-0xffffffff>}]}(1) | packet_content {offset_0-15 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_16-31 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> |offset_32-47 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_48-63 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> | offset_64-79 <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff> <hex 0x0-0xffffffff>}(1) |ipv6 {[{ class <value0-255>| flowlabel <hex 0x0-0xfffff>}| source_ipv6 <ipv6addr>| destination_ipv6 <ipv6addr>]}(1)] port [<portlist> | all][permit | deny] {time_range <range_name 32>}| delete access_id <value 1-100>]**
Description	This command is used to configure a CPU access profile for CPU Interface Filtering and to enter specific values that will be combined, using a logical AND operational method, with masks entered with the **config cpu access_profile** command, above.
Parameters	*profile_id <value 1-5>* – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. *add access_id <value 1-100>* – Adds an additional rule to the above specified access profile.

config cpu access_profile

The value is used to index the rule created.

ethernet – Specifies that the Switch will look only into the layer 2 part of each packet.

vlan <vlan_name 32>| *vlan_id <value 1-4094>* – Specifies that the access profile will apply to only to this VLAN.

source_mac <macaddr 000000000000-ffffffffffff > – Specifies that the access profile will apply to this source MAC address.

destination_mac <macaddr 000000000000-ffffffffffff > – Specifies that the access profile will apply to this destination MAC address.

ethernet_type <hex 0x0-0xffff> – Specifies that the access profile will apply only to packets with this hexadecimal 802.1Q Ethernet type value in the packet header.

ip – Specifies that the Switch will look into the IP fields in each packet.

vlan <vlan_name 32> | *vlan_id <value 1-4094>* – Specifies that the access profile will apply to only this VLAN.

source_ip <ipaddr> – Specifies that the access profile will apply to only packets with this source IP address.

destination_ip <ipaddr> – Specifies that the access profile will apply to only packets with this destination IP address.

dscp <value 0-63> – Specifies that the access profile will apply only to packets that have this value in their Type-of-Service (DiffServ code point, DSCP) field in their IP packet header

icmp – Specifies that the Switch will examine the Internet Control Message Protocol (ICMP) field within each packet.

- *type <value 0-255>* – Specifies that the access profile will apply to this ICMP type value.
- *code <value 0-255>* – Specifies that the access profile will apply to this ICMP code.

igmp – Specifies that the Switch will examine the Internet Group Management Protocol (IGMP) field within each packet.

- *type <value 0-255>* – Specifies that the access profile will apply to this IGMP type value.

tcp – Specifies that the Switch will examine the Transmission Control Protocol (TCP) field within each packet.

- *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP source port in their TCP header.
- *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this TCP destination port in their TCP header.
- *urg* | *ack* | *psh* | *rst* | *syn* | *fin* – Enters the appropriate flag_mask parameter. All incoming packets have TCP port numbers contained in them as the forwarding criterion. These numbers have flag bits associated with them which are parts of a packet that determine what to do with the packet. The user may deny packets by denying certain flag bits within the packets. The user may choose between urg (urgent), ack (acknowledgement), psh (push), rst (reset), syn (synchronize) and fin (finish).

udp – Specifies that the Switch will examine the User Datagram Protocol (UDP) field within each packet.

- *src_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this UDP source port in their UDP header.
- *dst_port <value 0-65535>* – Specifies that the access profile will apply only to packets that have this UDP destination port in their UDP header.

protocol_id <value 0-255> – Specifies that the Switch will examine the protocol field in each packet and if this field contains the value entered here, apply the following rules.

- *user_define_mask <hex 0x0-0xffffffff>* – Specifies that the rule applies to the IP protocol ID and the mask options behind the IP header.

packet_content_mask – Specifies that the Switch will mask the packet header beginning with

config cpu access_profile

	the offset value specified as follows: • *offset_0-15* – Enters a value in hex form to mask the packet from byte 0 to byte 15. • *offset_16-31* – Enters a value in hex form to mask the packet from byte 16 to byte 31. • *offset_32-47*– Enters a value in hex form to mask the packet from byte 32 to byte 47. • *offset_48-63* – Enters a value in hex form to mask the packet from byte 48 to byte 63. • *offset_64-79* – Enters a value in hex form to mask the packet from byte 64 to byte 79. *IPV6* – Denotes that IPv6 packets will be examined by the Switch for forwarding or filtering based on the rules configured in the **config access_profile** command for IPv6. • *class* – Entering this parameter will instruct the Switch to examine the *class* field of the IPv6 header. This class field is a part of the packet header that is similar to the Type of Service (ToS) or Precedence bits field in IPv4. • *flowlabel* – Entering this parameter will instruct the Switch to examine the *flow label* field of the IPv6 header. This flow label field is used by a source to label sequences of packets such as non-default quality of service or real time service packets. • *source_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the source IPv6 address. *destination_ipv6_mask <ipv6mask>* – Specifies an IP address mask for the destination IPv6 address. *permit* | *deny* – Specify that the packet matching the criteria configured with command will either be permitted or denied entry to the CPU. *time_range* – Specifies the time_range profile that has been associated with the ACL entries. *delete access_id <value 1-100>* – Use this to remove a previously created access rule in a profile ID.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure CPU access list entry:

```
DGS-3700-12:5#config cpu access_profile profile_id 5 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny
Command: config cpu access_profile profile_id 10 add access_id 1 ip vlan default
source_ip 20.2.2.3 destination_ip 10.1.1.252 dscp 3 icmp type 11 code 32 port 1 deny

Success.

DGS-3700-12:5#
```

show cpu access_profile

Purpose	Used to view the CPU access profile entry currently set in the Switch.
Syntax	**show cpu access_profile {profile_id <value 1-5>}**
Description	This command is used to view the current CPU interface filtering entries set on the Switch.
Parameters	*profile_id <value 1-5>* – Enter an integer between *1* and *5* that is used to identify the CPU access profile to be deleted with this command. This value is assigned to the access profile when it is created with the **create cpu access_profile** command.
Restrictions	None.

Example usage:

To show the CPU filtering state on the Switch:

```
DGS-3700-12:5#show cpu access_profile
Command: show cpu access_profile

CPU Interface Filtering State: Disabled

CPU Interface Access Profile Table

Total Unused Rule Entries:499
Total Used Rule Entries  :1


Access Profile ID: 1                                        Type : IP
================================================================================
MASK Option :
VLAN         Source IP Mask  Dst. IP Mask    DSCP ICMP Type Code
             20.0.0.0        10.0.0.0
-----------  --------------- --------------- ---- ----------------
--------------------------------------------------------------------------------

Access ID : 2              Mode: Deny
Ports: 1
-----------  --------------- --------------- ---- ----------------
VLAN name    Source IP       Dst. IP         DSCP ICMP Type Code
default      20.0.0.0        10.0.0.0        3         11   32

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

enable cpu_interface_filtering

Purpose	Used to enable CPU interface filtering on the Switch.
Syntax	**enable cpu_interface_filtering**
Description	This command is used in conjunction with the **disable cpu_interface_filtering** command below, to enable and disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To enable CPU interface filtering:

```
DGS-3700-12:5#enable cpu_interface_filtering
Command: enable cpu_interface_filtering

Success.

DGS-3700-12:5#
```

disable cpu_interface_filtering

Purpose	Used to disable CPU interface filtering on the Switch.
Syntax	**disable cpu_interface_filtering**

disable cpu_interface_filtering

Description	This command is used in conjunction with the **enable cpu_interface_filtering** command above to enable and disable CPU interface filtering on the Switch.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable CPU filtering:

```
DGS-3700-12:5#disable cpu_interface_filtering
Command: disable cpu_interface_filtering

Success.

DGS-3700-12:5#
```

config flow_meter

Purpose	Used to limit the bandwidth of the ingress traffic.
Syntax	**Config flow_meter [profile_id <value 1-12> | profile_name <name 1-32>] access_id <value 1-128>[[tr_tcm cir <value 0-15624> {cbs <value 0-16384>} pir <value 0-15624> {pbs <value 0-16384>}|sr_tcm cir <value 0-15624> cbs <value 0-16384> ebs <value 0-16384>] {conform permit {replace_dscp <value 0-63>} {counter [enable |disable]}} exceed [permit {replace_dscp <value 0-63>} {counter [enable |disable]} | drop] violate [permit {replace_dscp <value 0-63>} {counter [enable |disable]} | drop] |delete]**
Description	This command is used to limit the bandwidth of the ingress traffic. When the users create an ACL rule to filter packets, a metering rule can be created to associate with this ACL rule to limit traffic.
Parameters	*profile_id <value 1-12>* – Enter an integer used to identify the access profile that will be configured with this command. This value is assigned to the access profile when it is created with the **create access_profile** command. The profile ID sets the relative priority for the profile and specifies an index number that will identify the access profile being created with this command. Priority is set relative to other profiles where the lowest profile ID has the highest priority. The user may enter a profile ID number between 1 and 12. *profile_name <name 1-32>* – Specifies the name of the profile. The maximum length is 32 characters. *access_id <value 1-128>* – Adds an additional rule to the above specified access profile. The value is used to index the rule created. For information on number of rules that can be created for a given port, lease see the introduction to this chapter. *tr_tcm* – Specify the “two rate three color mode” cir <value 0-15624> – Specify the “committed information rate” The unit is 64Kbps. That is to say, 1 means 64Kbps. cbs <value 0-16384> – Specify the “committed burst size” 1. The unit is Kbyte. That is to say, 1 means 1Kbyte. 2. This parameter is an optional parameter. The default value is 4*1024. 3. The max set value is 16*1024. pir <value 0-15624> – Specify the “peak information rate” The unit is 64Kbps. That is to say, 1 means 64Kbps. pbs <value 0-16384> – Specify the “peak burst size” 1. The unit is Kbyte. That is to say, 1 means 1Kbyte. 2. This parameter is an optional parameter.The default value is 4*1024 3. The max set value is 16*1024.

config flow_meter

	sr_tcm – Specify the "single rate three color mode" cir <value 0-15624> – Specify the "committed information rate" The unit is 64Kbps. That is to say, 1 means 64Kbps. cbs <value 0-16384> – Specify the "committed burst size" 1. The unit is Kbyte. That is to say, 1 means 1Kbyte. 2. The max set value is 16*1024. ebs <value 0-16384> – Specify the "excess burst size" 1. The unit is Kbyte. That is to say, 1 means 1 Kbyte. 2. The max set value is 16*1024. *conform* - Specify the action when packet is in "green color" permit – Permit the packet. replace_dscp – Change the dscp of the packet. counter – Specify the counter. This is optional. The default is "disable". *exceed* – Specify the action when packet is in "yellow color" permit – Permit the packet. replace_dscp – Change the dscp of packet drop – Drop the packet. counter – Specify the counter. This is optional. The default is "disable". *violate* – Specify the action when packet is in "red color" Permit – Permit the packet. replace_dscp – Change the dscp of packet. counter – Specify the counter. This is optional. The default is "disable". *drop* – Specifies to drop the packet. The resource may be limited so that the counter can not be turned on. The limitation is project dependent. The counter will be cleared when the function is disabled. delete – Delete the specified flow_meter.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the ACL flow meter on the Switch:

```
DGS-3700-12:5#config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir
2000 pbs 2000 exceed permit replace_dscp 21 violate drop
Command: config flow_meter profile_id 1 access_id 1 tr_tcm cir 1000 cbs 200 pir 2000
pbs 2000 exceed permit replace_dscp 21 violate drop

Success.

DGS-3700-12:5#
```

show flow_meter

Purpose	Used to view the current state of ACL flow meter on the Switch.
Syntax	**show flow_meter { [profile_id < value 1-12> | profile_name <name 1-32>] { access_id < value 1-128>}}**
Description	This command is used to view the current state of ACL flow meter on the Switch.
Parameters	*profile_id <value 1-12>* – Specifies the profile_ID *profile_name <name 1-32>*– Specifies the name of the profile. The maximum length is 32 characters.

show flow_meter

	access_id <value 1-128> – Specifies the access_ID
Restrictions	None.

Example usage:

To show the ACL flow meter state on the Switch:

```
DGS-3700-12:5#show flow_meter
Command: show flow_meter

Flow Meter Information:
------------------------------------------------------------------------
Profile ID : 1     Access ID : 1      Mode : trTCM
CIR(64Kbps):1000   CBS(Kbyte):2000   PIR(64Kbps):2000   PBS(Kbyte):2000
Action:
       Conform : Permit    Replace DSCP : 11     Counter : Enabled
       Exceed  : Permit    Replace DSCP : 22     Counter : Enabled
       Violate : Drop                            Counter : Disabled
------------------------------------------------------------------------

Profile ID : 1     Access ID : 2      Mode : srTCM
CIR(64Kbps):2500     CBS(Kbyte):2000    EBS(Kbyte):3500
Action:
      Conform : Permit     Replace DSCP:          Counter : Enabled
      Exceed  : Permit     Replace DSCP: 33       Counter : Enabled
      Violate : Drop                              Counter : Disabled
------------------------------------------------------------------------

Total Entries: 2
DGS-3700-12:5#
```

config time_range

Purpose	Used to configure the range of time to activate a function on the switch.
Syntax	**config time_range <range_name 32> [hours start_time < time hh:mm:ss > end_time< time hh:mm:ss > weekdays <daylist> | delete]**
Description	This command defines a specific range of time to activate a function on the Switch by specifying which time range in a day and which days in a week are covered in the time range. Note that the specified time range is based on SNTP time or configured time. If this time is not available, then the time range will not be met.
Parameters	*range_name* – Specifies the name of the time range settings. *start_time* – Specifies the starting time in a day. (24-hr time) For example, 19:00 means 7PM. 19 is also acceptable. start_time must be smaller than end_time. *end_time* – Specifies the ending time in a day. (24-hr time) *weekdays* – Specify the list of days contained in the time range. Use a dash to define a period of days. Use a comma to separate specific days. For example, mon-fri (Monday to Friday) sun, mon, fri (Sunday, Monday and Friday) *delete* – Deletes a time range profile. When a time_range profile has been associated with ACL entries, the delete of this time_range profile will fail.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To config time range:

```
DGS-3700-12:5#config time_range 1-3_new hours start_time 11:21:20 end_time 11:44:40 
weekdays mon-fri
Command: config time_range 1-3_new hours start_time 11:21:20 end_time 11:44:40 
weekdays mon-fri

Success.

DGS-3700-12:5#
```

show time_range

Purpose	Used to display current access list table.
Syntax	**show time_range**
Description	This command is used to display current time range setting.
Parameters	None.
Restrictions	None.

Example usage:

To show the time range on the Switch:

```
DGS-3700-12:5#show time_range
Command: show time_range

Time Range Information
-------------------------
Range Name   :  1-3_new
Weekdays     :  Mon,Tue,Wed,Thu,Fri
Start Time   :  11:21:20
End Time     :  11:44:40

Total Entries :1

DGS-3700-12:5#
```

show current_config access_profile

Purpose	This command displays the ACL part of current configuration.
Syntax	**show current_config access_profile**
Description	This command displays the ACL privilege of the current configuration in user level of privilege. The overall current configuration can be displayed by show config command which is accessible in administrator level of privilege.
Parameters	None.
Restrictions	None.

Example usage:

To show the current configuration access profile on the Switch:

```
DGS-3700-12:5#show current_config access_profile
Command: show current_config access_profile

#-----------------------------------------------------------------

# ACL

create access_profile profile_id 1 profile_name RG ethernet vlan ethernet_type

#-----------------------------------------------------------------

DGS-3700-12:5#
```

57

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	Parameters
show packet ports	<portlist>
show error ports	<portlist>
show utilization	[cpu | ports {<portlist>}]
show utilization dram	
show utilization flash	
clear counters	{ports <portlist>}
show historical_counter	[packet | error] [ports <portlist>] [15_minute {slot <index 1-5>} | 1_day { slot <index 1-2> }]
show historical_utilization	[cpu | memory] [15_minute { slot <index 1-5> } | 1_day { slot <index 1-2>}]
clear historical_counters ports	[<portlist> | all]
clear log	
show log	{index <value_list> }
enable syslog	
disable syslog	
show syslog	
create syslog host	<index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number>| state [enable | disable]
config syslog host	[all | <index 1-4>] {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]}
delete syslog host	[<index 1-4> | all]
show syslog host	{<index 1-4>}
config log_save_timing	[time_interval <min 1-65535> | on_demand | log_trigger]
show log_save_timing	
show attack_log	{index <value_list>}
clear attack_log	
upload attack_log_toTFTP	[<ipaddr>|<ipv6addr>] <path_filename 64>
config system_severity	[trap | log | all] [critical | warning | information]
show system_severity	

Each command is listed, in detail, in the following sections.

show packet ports

Purpose	Used to display statistics about the packets sent and received by the Switch.
Syntax	**show packet ports <portlist>**
Description	This command is used to display statistics about packets sent and received by ports specified in the *<portlist>*.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the packets analysis for port 2:

```
DGS-3700-12:5#show packet port 2
Command: show packet port 2

Port Number : 2
 ================================================================
 Frame Size/Type       Frame Counts                Frames/sec
 --------------        ----------------------      -----------
 64                    0                           0
 65-127                0                           0
 128-255               0                           0
 256-511               0                           0
 512-1023              0                           0
 1024-1518             0                           0
 Unicast RX            0                           0
 Multicast RX          0                           0
 Broadcast RX          0                           0

 Frame Type            Total                       Total/sec
 --------------        ----------------------      -----------
 RX Bytes              0                           0
 RX Frames             0                           0
 TX Bytes              0                           0
 TX Frames             0                           0

DGS-3700-12:5#
```

show error ports

Purpose	Used to display the error statistics for a range of ports.
Syntax	**show error ports <portlist>**
Description	This command will display all of the packet error statistics collected and logged by the Switch for a given port list.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the errors of the port 3:

```
DGS-3700-12:5#show error ports 3
Command: show error ports 3

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

DGS-3700-12:5#
```

show utilization

Purpose	Used to display real-time port and CPU utilization statistics.
Syntax	**show utilization [cpu | ports {<portlist>}]**
Description	This command will display the real-time port and CPU utilization statistics for the Switch.
Parameters	*cpu* – Entering this parameter will display the current cpu utilization of the Switch. *ports* – Entering this parameter will display the current port utilization of the Switch. • *<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To display the port utilization statistics:

```
DGS-3700-12:5#show utilization ports
Command: show utilization ports

Port     TX/sec     RX/sec   Util
 -----  ---------- ---------- ----
 1      0          0          0
 2      0          0          0
 3      31         0          1
 4      0          0          0
 5      0          0          0
 6      0          0          0
 7      2          32         1
 8      0          0          0
 9      0          0          0
 10     0          0          0
 11     0          0          0
 12     0          0          0

DGS-3700-12:5#
```

To display the current CPU utilization:

```
DGS-3700-12:5#show utilization cpu
Command: show utilization cpu

CPU Utilization
-------------------------------------------------------------
Five seconds -   9 %   One minute -  10 %    Five minutes -  10 %

DGS-3700-12:5#
```

show utilization dram

Purpose	Used to display real-time utilization statistics for the DRAM.
Syntax	**show utilization dram**
Description	This command will display the real-time utilization statistics for the DRAM on the Switch.
Parameters	None.
Restrictions	None.

To display the current utilization of DRAM:

```
DGS-3700-12:5#show utilization dram
Command: show utilization dram

DRAM utilization :
        Total DRAM      : 131072    KB
        Used DRAM       : 123879    KB
        Utilization     : 94 %

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

show utilization flash

Purpose	Used to display real-time utilization statistics for the flash memory.
Syntax	**show utilization flash**
Description	This command will display the real-time utilization statistics for the flash memory on the Switch.
Parameters	None.
Restrictions	None.

To display the current utilization of flash:

```
DGS-3700-12:5#show utilization flash
Command: show utilization flash

FLASH Memory Utilization :
        Total FLASH     : 32768     KB
        Used FLASH      : 8688      KB
        Utilization     : 26 %

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

clear counters

Purpose	Used to clear the Switch's statistics counters.
Syntax	**clear counters {ports <portlist>}**
Description	This command will clear the counters used by the Switch to compile statistics.
Parameters	*<portlist>* – Specifies a port or range of ports to be displayed.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the counters:

```
DGS-3700-12:5#clear counters ports 2-9
Command: clear counters ports 2-9

Success.

DGS-3700-12:5#
```

show historical_counter

Purpose	Used to display statistics about the packets sent and received by the switch.
Syntax	**show historical_counter [packet | error] [ports <portlist>] [15_minute {slot <index 1-5>} | 1_day { slot <index 1-2> }]**
Description	This command is used to display statistics about the packets sent and received by the switch. For 15 minute counters, five historical statistic entries are supported. Users can select which entry to show. For statistics based on a day, only two historical statistic entries are supported.
Parameters	*packet* – Displays valid packets. *error* – Displays error packets. *portlist* – Specifies a range of ports to be shown. *15_minute* – Specifies to display 15-minute based statistics count. If there is no option specified, all 15 minutes time slots will be displayed. *1_day* – Specifies to display daily based statistics count. If there is no option specified, all 1-day time slots will be displayed. *slot* – Specifies the slot number to display.
Restrictions	None.

Example usage:

To show the statistic count of packets for current 15_minute slots:

```
DGS-3700-12:5#show historical_counter packet ports 1 15_minute slot 1
Command: show historical_counter packet ports 1 15_minute slot 1

 Port 1 15-Minute Slot 1 :

 Starttime : 7 Jan 2009  20:13:32
 Endtime   : 7 Jan 2009  19:58:32

 Frame Size/Type      Frame Count
 -------------        -----------
 Pkts TX              0
```

```
Bytes TX              0
Pkts RX               0
Bytes RX              0
64 RX                 0
65-127 RX             0
128-255 RX            0
256-511 RX            0
512-1023 RX           0
1024-1518 RX          0
Unicast RX            0
Multicast RX          0
Broadcast RX          0

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

show historical_utilization

Purpose	Used to display the utilization of the cpu and the memory.
Syntax	**show historical_utilization [cpu | memory] [15_minute { slot <index 1-5> } | 1_day { slot <index 1-2>}]**
Description	This command is used to show the historical utilization of the cpu and the memory. For 15 minutes cpu or memory utilization, five historical statistic entries are supported. Users can select which entry to show. For statistics based on a day, only two historical statistic entries are supported.
Parameters	*cpu* – Displays the utilization of cpu. *memory* – Displays the utilization of memory. *15_minute* – Displays the 15 min based statistics count. If there is no option specified, all 15 minutes time slots will be displayed. *1_day* – Specifies to display daily based statistics count. If there is no option specified, all 1-day time slots will be displayed. *slot* – Specify the slot number to display.
Restrictions	None.

Example usage:

To show the cpu utilization of the five most recent 15 minute statistic count:

```
DGS-3700-12:5#show historical_utilization cpu 15_minute
Command: show historical_utilization cpu 15_minute

CPU Utilization
-------------------------------------------------------------------------
15-Minute Slot 1 (7 Jan 2009  20:25:01 - 7 Jan 2000  20:10:01)  :  10 %
15-Minute Slot 2 (7 Jan 2009  20:10:01 - 7 Jan 2000  19:55:01)  :  10 %
15-Minute Slot 3 (7 Jan 2009  19:54:59 - 7 Jan 2000  19:39:59)  :  11 %
15-Minute Slot 4 (7 Jan 2009  19:39:59 - 7 Jan 2000  19:24:59)  :   0 %
15-Minute Slot 5 (7 Jan 2009  19:24:59 - 7 Jan 2000  19:09:59)  :   0 %

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

To show the cpu utilization of the two most recent 1 day statistic count:

```
DGS-3700-12:5#show historical_utilization cpu 1_day
Command: show historical_utilization cpu 1_day

CPU Utilization
-------------------------------------------------------------------------
1-Day Slot 1 (7 Jan 2009  20:27:51 - 6 Jan 2000  20:27:51)  :  10 %
1-Day Slot 2 (6 Jan 2009  20:27:51 - 5 Jan 2000  20:27:51)  :   0 %

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

To show the cpu utilization of the current 1 day statistic count:

```
DGS-3700-12:5# show historical_utilization memory 1_day slot 1
show historical_utilization memory 1_day slot 1

Memory Utilization

Starttime : 7 Jan 2009  20:29:47
Endtime   : 6 Jan 2009  20:29:47
-------------------------------------------------------------------------
1-Day Slot 1        :  93 %

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

clear historical_counters ports

Purpose	Used to clear port historical counter statistics.
Syntax	**clear historical_counters ports [<portlist> | all]**
Description	This command is used to delete port counter statistics.
Parameters	*<portlist>* – Specifies a port or range of ports to be cleared. *all* – All ports will be cleared.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the historical counter for all ports:

```
DGS-3700-12:5#clear historical_counters ports all
Command: clear historical_counters ports all

Success.

DGS-3700-12:5#
```

clear log

Purpose	Used to clear the Switch's history log.
Syntax	**clear log**
Description	This command is used to clear the Switch's history log.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the log information:

```
DGS-3700-12:5#clear log
Command: clear log

Success.

DGS-3700-12:5#
```

show log

Purpose	Used to display the switch history log.
Syntax	**show log {index <value_list>}**
Description	This command is used to display the contents of the Switch's history log.
Parameters	*index <value_list>* – This parameter specifies the range of log index to show. For example, show log index 1-5 will display the history log from 1 to 5. If no parameter is specified, all history log entries will be displayed.
Restrictions	None.

Example usage:

To display the switch history log**:**

```
DGS-3700-12:5#show log index 1-5
Command: show log index 1-5

Index Date       Time     Log Text
----- ---------- -------- ---------------------------------------------------
5     2000-01-03 18:53:06 Logout through Console (Username: Anonymous)
4     2000-01-03 18:47:22 Successful login through Console (Username: Anonymous)
3     2000-01-03 18:47:18 Port 3 link up, 1000Mbps FULL duplex
2     2000-01-03 18:47:18 Port 7 link up, 100Mbps FULL duplex
1     2000-01-03 18:47:18 System started up

DGS-3700-12:5#
```

NOTE: For detailed information regarding Log entries that will appear in this window, please refer to Appendix C at the back of the ***DGS-3700-12 Layer 2 Gigabit Ethernet Managed Switch User Manual.***

enable syslog

Purpose	Used to enable the system log to be sent to a remote host.
Syntax	**enable syslog**
Description	This command is used to enable the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To the Syslog function on the Switch:

```
DGS-3700-12:5#enable syslog
Command: enable syslog

Success.

DGS-3700-12:5#
```

disable syslog

Purpose	Used to disable the system log to be sent to a remote host.
Syntax	**disable syslog**
Description	This command is used to disable the system log to be sent to a remote host.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To disable the syslog function on the Switch:

```
DGS-3700-12:5#disable syslog
Command: disable syslog

Success.

DGS-3700-12:5#
```

show syslog

Purpose	Used to display the syslog protocol status as enabled or disabled.
Syntax	**show syslog**
Description	This command is used to display the syslog status as enabled or disabled.
Parameters	None.
Restrictions	None.

Example usage:

To display the current status of the syslog function:

```
DGS-3700-12:5#show syslog
Command: show syslog

Syslog Global State: Enabled

DGS-3700-12:5#
```

create syslog host

Purpose	Used to create a new syslog host.
Syntax	**create syslog host <index 1-4> ipaddress <ipaddr> {severity [informational | warning | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | state [enable | disable]**
Description	This command is used to create a new syslog host.

create syslog host

Parameters

<index 1-4> – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.

ipaddress <ipaddr> – Specifies the IP address of the remote host where syslog messages will be sent.

severity – Severity level indicator. These are described in the following:

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

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 will be sent to the remote host. This corresponds to number 16 from the list above.

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

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

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

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

local5 – Specifies that local use 5 messages will be sent to the remote host. This

create syslog host

	corresponds to number 21 from the list above. *local6* – Specifies that local use 6 messages will be sent to the remote host. This corresponds to number 22 from the list above. *local7* – Specifies that local use 7 messages will be sent to the remote host. This corresponds to number 23 from the list above. *udp_port <udp_port_number>* – Specifies the UDP port number that the syslog protocol will 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 and Operator-level users can issue this command.

Example usage:

To create a Syslog host:

```
DGS-3700-12:5#create syslog host 1 severity all facility local0 ipaddress 1.1.1.1

Command: create syslog host 1 severity all facility local0 ipaddress 1.1.1.1

Success.

DGS-3700-12:5#
```

config syslog host

Purpose	Used 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 | all] | facility [local0 | local1 | local2 | local3 | local4 | local5 | local6 | local7] | udp_port <udp_port_number> | ipaddress <ipaddr> | state [enable | disable]**
Description	This command is used to configure the syslog protocol to send system log information to a remote host.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *ipaddress <ipaddr>* – Specifies the IP address of the remote host where syslog messages will be sent. *severity* – Severity level indicator. These are described in the following: **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 will be sent to the remote host. This corresponds to number 6 from the list above.

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

all – Specifies that all of the currently supported syslog messages that are generated by the Switch will 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 the Switch currently supports.

Parameters

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 will be sent to the remote host. This corresponds to number 16 from the list above.

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

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

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

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

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

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

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

udp_port <udp_port_number> – Specifies the UDP port number that the syslog protocol will 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 and Operator-level users can issue this command.

Example usage:

To configure a Syslog host:

```
DGS-3700-12:5#config syslog host 1 severity all
Command: config syslog host 1 severity all
Success.

DGS-3700-12:5#
```

Example usage:

To configure a syslog host for all hosts:

```
DGS-3700-12:5#config syslog host all severity all
Command: config syslog host all severity all
Success.

DGS-3700-12:5#
```

delete syslog host

Purpose	Used to remove a syslog host that has been previously configured, from the Switch.
Syntax	**delete syslog host [<index 1-4> | all]**
Description	This command is used to remove a syslog host that has been previously configured from the Switch.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4. *all* – Specifies that the command will be applied to all hosts.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To delete a previously configured syslog host:

```
DGS-3700-12:5#delete syslog host 4
Command: delete syslog host 4

Success.

DGS-3700-12:5#
```

show syslog host

Purpose	Used to display the syslog hosts currently configured on the Switch.
Syntax	**show syslog host {<index 1-4>}**
Description	This command is used to display the syslog hosts that are currently configured on the Switch.
Parameters	*<index 1-4>* – Specifies that the command will be applied to an index of hosts. There are four available indexes, numbered 1 through 4.
Restrictions	None.

Example usage:

To show Syslog host information:

```
DGS-3700-12:5#show syslog host
Command: show syslog host

Syslog Global State: Disabled

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

Total Entries : 3

DGS-3700-12:5#
```

config log_save_timing

Purpose	Used to configure the method to save log.
Syntax	**config log_save_timing [time_interval <min 1-65535> | on_demand | log_trigger]**
Description	This command is used to set the method to save log.
Parameters	*time_interval* – save log to flash every xxx minutes. (if no log happen in this period, don't save) *on_demand* – save log to flash whenever user type "save log" or "save all" This is also the default. *log_trigger* – save log to flash whenever log arrives
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure log_save_timing:

```
DGS-3700-12:5#config log_save_timing on_demand
Command: config log_save_timing on_demand

Success.

DGS-3700-12:5#
```

show log_save_timing

Purpose	Used to show the timing method to save log.
Syntax	**show log_save_timing**
Description	This command is used to show method to save log.
Parameters	None.
Restrictions	None.

Example usage:

To show log_save_timing:

```
DGS-3700-12:5#show log_save_timing
Command: show log_save_timing

Saving Log Method: On_demand


DGS-3700-12:5#
```

show attack_log

Purpose	Used to show dangerous log messages.
Syntax	**show attack_log {index <value_list>}**
Description	This command is used to show content of dangerous log messages.
Parameters	*value_list X-Y* – The show log command will display the dangerous log messages between the log number of X and Y. For example, show dangerous log index 1-5 will display the dangerous log messages from 1 to 5. If no parameter specified, all dangerous log entries will be displayed.
Restrictions	None.

Example usage:

To show dangerous messages on master:

```
DGS-3700-12:5#show attack_log
Command: show attack_log

Index  Time                Log Text
----   --------------      ----------------------
2      00000 days 01:25:43  Possible spoofing attack from 000d01002301 port 6
1      00000 days 01:25:43  Possible spoofing attack from 000d01002301 port 6

DGS-3700-12:5#
```

clear attack_log

Purpose	Used to clear the switch's dangerous log.
Syntax	**clear attack_log**
Description	This command is used to clear the switch's dangerous log.
Parameters	None.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To clear the master's dangerous log:

```
DGS-3700-12:5#clear attack_log
Command: clear attack_log

Success.

DGS-3700-12:5#
```

upload attack_log_to TFTP

Purpose	Used to upload the switch's dangerous log.
Syntax	**upload attack_log_toTFTP [<ipaddr>|<ipv6addr> <path_filename 64>**
Description	This command is used to upload the switch's dangerous log.
Parameters	*<ipaddr>* – The IP address of the TFTP server. The TFTP server must be on the same IP subnet as the switch. *<path_filename 64>* – Specifies the location of the file on the TFTP server. The uploaded file from the switch will replace this file.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To upload the master's dangerous log:

```
DGS-3700-12:5#upload attack_log_toTFTP 10.90.90.1 C:\alert.txt
Command: upload attack_log_toTFTP 10.90.90.1 C:\alert.txt

Success.

DGS-3700-12:5#
```

config system_severity

Purpose	To configure system_severity level of an alert required for log entry or trap message.
Syntax	**config system_severity [trap | log | all] [critical | warning | information]**
Description	This command is used to configure the system_severity levels on the Switch. When an event occurs on the Switch, a message will be sent to the SNMP agent (trap), the Switch's log or both. Events occurring on the Switch are separated into three main categories, these categories are NOT precisely the same as the parameters of the same name (see below). • Information – Events classified as information are basic events occurring on the Switch that are not deemed as problematic, such as enabling or disabling various functions on the Switch. • Warning – Events classified as warning are problematic events that are not critical to the overall function of the Switch but do require attention, such as unsuccessful downloads or uploads and failed logins. • Critical – Events classified as critical are fatal exceptions occurring on the Switch, such as hardware failures or spoofing attacks.
Parameters	Choose one of the following to identify where severity messages are to be sent. • *trap* – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent for analysis. • *log* – Entering this parameter will define which events occurring on the Switch will be sent to the Switch's log for analysis. • *all* – Entering this parameter will define which events occurring on the Switch will be sent to a SNMP agent and the Switch's log for analysis. Choose one of the following to identify what level of severity warnings are to be sent to the destination entered above. *critical* – Entering this parameter along with the proper destination, stated above, will

config system_severity

	instruct the Switch to send only critical events to the Switch's log or SNMP agent. *warning* – Entering this parameter along with the proper destination, stated above, will instruct the Switch to send critical and warning events to the Switch's log or SNMP agent. *information* – Entering this parameter along with the proper destination, stated above, will instruct the switch to send informational, warning and critical events to the Switch's log or SNMP agent.
Restrictions	Only Administrator and Operator-level users can issue this command.

Example usage:

To configure the system severity settings:

```
DGS-3700-12:5#config system_severity trap critical
Command: config system_severity trap critical

Success.

DGS-3700-12:5#
```

show system_severity

Purpose	To display system_severity level of an alert required for log entry or trap message.
Syntax	**show system_severity**
Description	This command is used to display system_severity level of an alert required for log entry or trap message.
Parameters	None.
Restrictions	None.

Example usage:

To display the system severity settings for critical traps and log:

```
DGS-3700-12:5#show system_severity
Command: show system_severity

System Severity Trap : information
System Severity Log : information

DGS-3700-12:5#
```

58

CABLE DIAGNOSTIC COMMANDS

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

Command	Parameters
cable diagnostic	cable_diag ports [<portlist>|all]

Each command is listed, in detail, in the following sections.

cable diagnostic

Purpose	This command is used to diagnose the copper cable. If there is an error on the cable, it can determine the type of error and the position where the error occurred.
Syntax	**cable_diag ports [<portlist>|all]**
Description	When a port is in link up status, the diagnostic will obtain the distance of the cable. Since the status is link-up, the cable will not have any problem. Since this diagnostic is for copper cable, the port with fiber cable will be skipped from the diagnostic. If the link is up, the abnormal results won't be shown and the cable length item indicates the length of the cable. If the link is down the reason may be that its partner has powered off or the port is disabled, the abnormal results won't be shown and the cable length item shows the length of the cable. If the link is down and there is some error in the cable, the abnormal results will be shown, but the cable length item won't be shown.
Parameters	*all – Indicate all ports will be displayed.* <*portlist*> – Specifies a port or range of ports to be displayed.
Restrictions	None.

Example usage:

To do the cable diagnostic on ports 1-7 on the Switch:

```
DGS-3700-12:5#DGS-3700-12:5#cable_diag ports 1-7
Command: cable_diag ports 1-7

 Perform Cable Diagnostics ...

 Port   Type      Link Status          Test Result          Cable Length (M)
 ----  -------  --------------  -------------------------  ----------------
  1      GE        Link Down     No Cable                          -
  2      GE        Link Down     No Cable                          -
  3      GE        Link Up       OK                               55
  4      GE        Link Down     No Cable                          -
  5      GE        Link Down     No Cable                          -
  6      GE        Link Down     No Cable                          -
  7      GE        Link Up       OK                                5

DGS-3700-12:5#
```

59

PASSWORD RECOVERY COMMAND LIST

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

Command	Parameters
reset config	{force_agree}
reboot	{force_agree}
reset account	
reset password	{<username>}
show account	

Each command is listed, in detail, in the following sections.

NOTE: All Password revovery commands can be executed in password revovery mode. If you wish to enter the Switch into password recovery mode, simply press " ^ "after the system has booted up successfully and loaded the runtime image to 100%.

```
Boot Procedure                                              V1.00.B006
-----------------------------------------------------------------------
Power On Self Test.................................100%
MAC Address : 00-80-C2-11-22-00
H/W Version : A1
Please wait, loading V1.00.B035 Runtime image......100%

Password Recovery Mode
>_
```

reset config

Purpose	Used to reset the configuration .
Syntax	**reset config { force_agree }**
Description	This command is used to reset the configuration parameters. The configuration is reset but not saved.
Parameters	*force_agree*: if this parameter is specified, there will not be the prompt message to ask for user's confirmation.
Restrictions	None.

Example usage:

To reset the configuration:

```
>reset config
Command: reset config

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

reboot

Purpose	Used to exit Reset Configuration Mode and restart the switch.
Syntax	**reboot { force_agree }**
Description	This command is used to exit the Reset Configuration Mode and restarts the switch. And it pops out a confirmation message to save the current setting.
Parameters	*force_agree* – If this parameter is specified, there will not be the prompt message to ask for user's confirmation.
Restrictions	None.

Example usage:

To reboot:

```
>reboot
Command: reboot

Save current setting before system restart?(y/n)y

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

reset account

Purpose	Used to delete the created account.
Syntax	**reset account**
Description	This command is used to delete all of the created user accounts. The banner messages for password recover mode is: Password Recovery Mode
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset or delete an account:

```
>reset account
Command: reset account

Success
```

reset password

Purpose	Used to reset the password for user account
Syntax	**reset password {<username>}**
Description	This command is used to reset the password of the specified user to empty. If username is not specified, password of all users will be reset.
Parameters	None.
Restrictions	This command is only available in password recovery mode.

Example usage:

To reset the password:

```
>reset password
Command: reset password

Success
```

show account

Purpose	Used to show the created account.
Syntax	**show account**
Description	This command is used to display all already created accounts.
Parameters	None.
Restrictions	None.

Example usage:

To view the created account:

```
>show account
Command: show account

Current Accounts:
Username         Password        Access Level
---------------  --------        ------------
admin            (Empty)         Admin
user1            (Empty)         user

Total Entries : 2
```

60

COMMAND HISTORY LIST

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

Command	Parameters
?	
config command_history	<value 1-40>
show command_history	

Each command is listed, in detail, in the following sections.

?	
Purpose	Used to display all commands in the Command Line Interface (CLI).
Syntax	**? {<command>}**
Description	This command will display all of the commands available through the Command Line Interface (CLI).
Parameters	*{<command>}* – Entering the question mark with an appropriate command will list all the corresponding parameters for the specified command, along with a brief description of the commands 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-3700-12:5#?
Command: ?
..
?
cable_diag ports
cfm linktrace
cfm loopback
clear
clear address_binding dhcp_snoop binding_entry ports
clear arptable
clear attack_log
clear cfm pkt_cnt
clear counters
clear ethernet_oam ports
clear fdb
clear historical_counters ports
clear igmp_snooping data_driven_group
clear igmp_snooping statistic counter
clear log
clear mac_based_access_control auth_mac
clear mld_snooping data_driven_group
clear mld_snooping statistic counter
clear port_security_entry
clear vlan_counter statistics
```

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

To display the parameters for a specific command:

```
DGS-3700-12:5#? config stp
Command: ? config stp

Command: config stp
Usage:  {maxage <value 6-40>|maxhops <value 1-20> |hellotime <value 1-2>|
forwarddelay <value 4-30>|txholdcount <value 1-10>|fbpdu
[enable|disable]|nni_bpdu_addr [dot1d | dot1ad]}
Description: Used to update the STP Global Configuration.
config stp instance_id
config stp mst_config_id
config stp mst_ports
config stp ports
config stp priority
config stp version

DGS-3700-12:5#
```

config command_history

Purpose	Used to configure the command history.
Syntax	**config command_history <value 1-40>**
Description	This command is used to configure number of the executed command to be recorded in CLI.
Parameters	*<value 1-40>* – The number of previously executed commands maintained in the buffer. Up to 40 of the latest executed commands may be viewed.
Restrictions	None.

Example usage:

To configure the command history:

```
DGS-3700-12:5#config command_history 20
Command: config command_history 20

Success.

DGS-3700-12:5#
```

show command_history

Purpose	Used to display the command history.
Syntax	**show command_history**
Description	This command is used to display currently used command history.
Parameters	None.
Restrictions	None.

Example usage:

To display the command history:

```
DGS-3700-12:5#show command_history
Command: show command_history

config command_history 20
? config stp
?

DGS-3700-12:5#
```

Appendix A

MITIGATING ARP SPOOFING ATTACKS VIA PACKET CONTENT ACL

Address Resolution Protocol (ARP) is the standard method for finding a host's hardware address (MAC address) when only its IP address is known. This protocol is vulnerable because it can spoof the IP and MAC information in the ARP packets to attack a LAN (known as ARP spoofing). This section is intended to introduce ARP protocol, ARP spoofing attacks, and the counter measure brought by D-Link's switches to counter the ARP spoofing attack.

- ***How Address Resolution Protocol works***

In the process of ARP, PC A will, firstly, issue an ARP request to query PC B's MAC address. The network structure is shown in Figure-1.

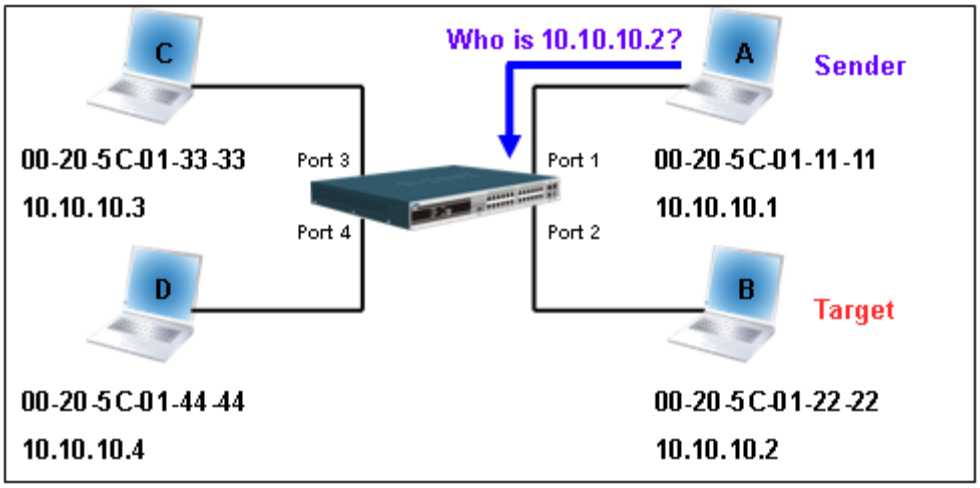


Figure – 1

In the mean time, PC A's MAC address will be written into the "Sender H/W Address" and its IP address will be written into the "Sender Protocol Address" in ARP payload. As PC B's MAC address is unknown, the "Target H/W Address" will be "00-00-00-00-00-00" while PC B's IP address will be written into the "Target Protocol Address", shown in Table-1.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP request	00-20-5C-01-11-11	***10.10.10.1***	***00-00-00-00-00-00***	***10.10.10.2***

Table – 1 (ARP Payload)

The ARP request will be encapsulated into Ethernet frame and sent out. As can be seen in Table-2, the "Source Address" in the Ethernet frame will be PC A's MAC address. Since an ARP request is sent via a broadcast, the "Destination address" is in the format of an Ethernet broadcast (FF-FF-FF-FF-FF-FF).

Destination address	Source address	Ether-type	ARP	FCS
FF-FF-FF-FF-FF-FF	***00-20-5C-01-11-11***			

Table – 2 (Ethernet frame format)

When the switch receives the frame, it will check the "Source Address" in the Ethernet frame's header. If the address is not in its Forwarding Table, the switch will learn PC A's MAC and the associated port into its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11

In addition, when the switch receives the broadcast ARP request, it will flood the frame to all ports except the source port, port 1 (see Figure -2).

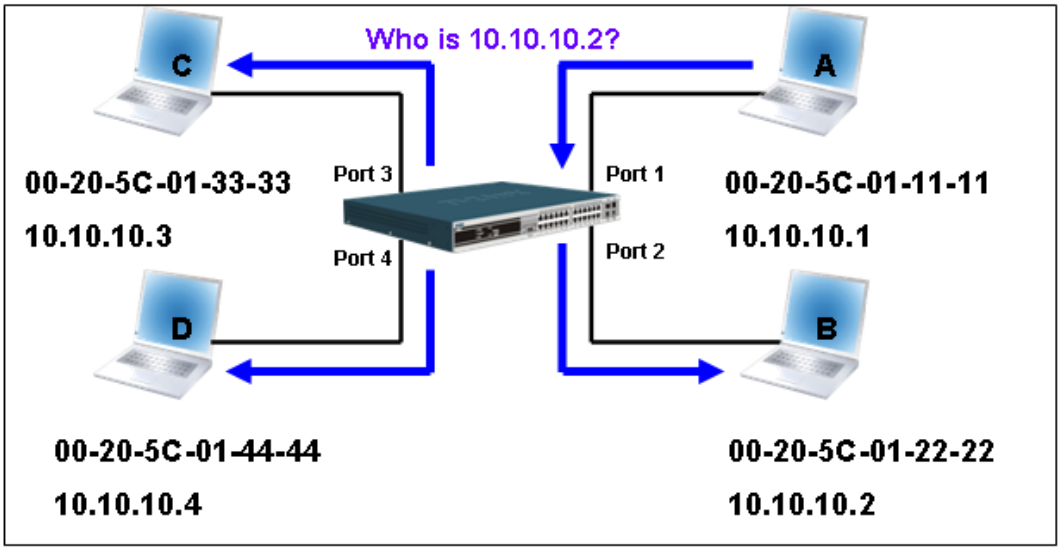


Figure – 2

When the switch floods the frame of ARP requests to the network, all PCs will receive and examine the frame but only PC B will reply to the query as the destination IP address of PC B matches (see Figure-3).

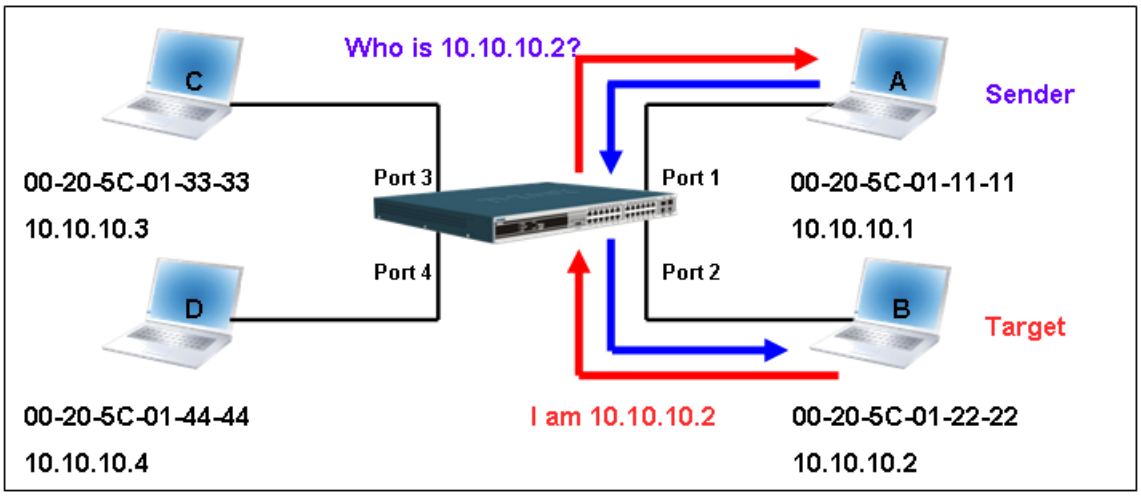


Figure – 3

When PC B replies to the ARP request, its MAC address will be written into “Target H/W Address” in the ARP payload shown in Table-3. The ARP reply will be then encapsulated into the Ethernet frame again and sent back to the sender. The ARP reply is in a form of Unicast communication.

H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
				ARP reply	***00-20-5C-01-11-11***	***10.10.10.1***	***00-20-5C-01-22-22***	***10.10.10.2***

Table – 3 (ARP Payload)

When PC B replies the query, the “Destination Address” in the Ethernet frame will be changed to PC A’s MAC address. The “Source Address” will be changed to PC B’s MAC address (see Table-4).

Destination address	Source address	Ether-type	ARP	FCS
00-20-5C-01-11-11	***00-20-5C-01-22-22***			

Table – 4 (Ethernet frame format)

The switch will also examine the “Source Address” of the Ethernet frame and find that the address is not in the Forwarding Table. The switch will learn PC B’s MAC and update its Forwarding Table.

Forwarding Table

Port1 00-20-5C-01-11-11
Port2 00-20-5C-01-22-22

- ***How ARP spoofing attacks a network***

ARP spoofing, also known as ARP poisoning, is a method to attack an Ethernet network which may allow an attacker to sniff data frames on a LAN, modify the traffic, or stop the traffic altogether (known as a Denial of Service - DoS attack). The principle of ARP spoofing is to send the fake, or spoofed ARP messages to an Ethernet network. Generally, the aim is to associate the attacker's or random MAC address with the IP address of another node (such as the default gateway). Any traffic meant for that IP address would be mistakenly re-directed to the node specified by the attacker.

IP spoofing attack is caused by Gratuitous ARP that occurs when a host sends an ARP request to resolve its own IP address. Figure-4 shows a hacker within a LAN to initiate ARP spoofing attack.

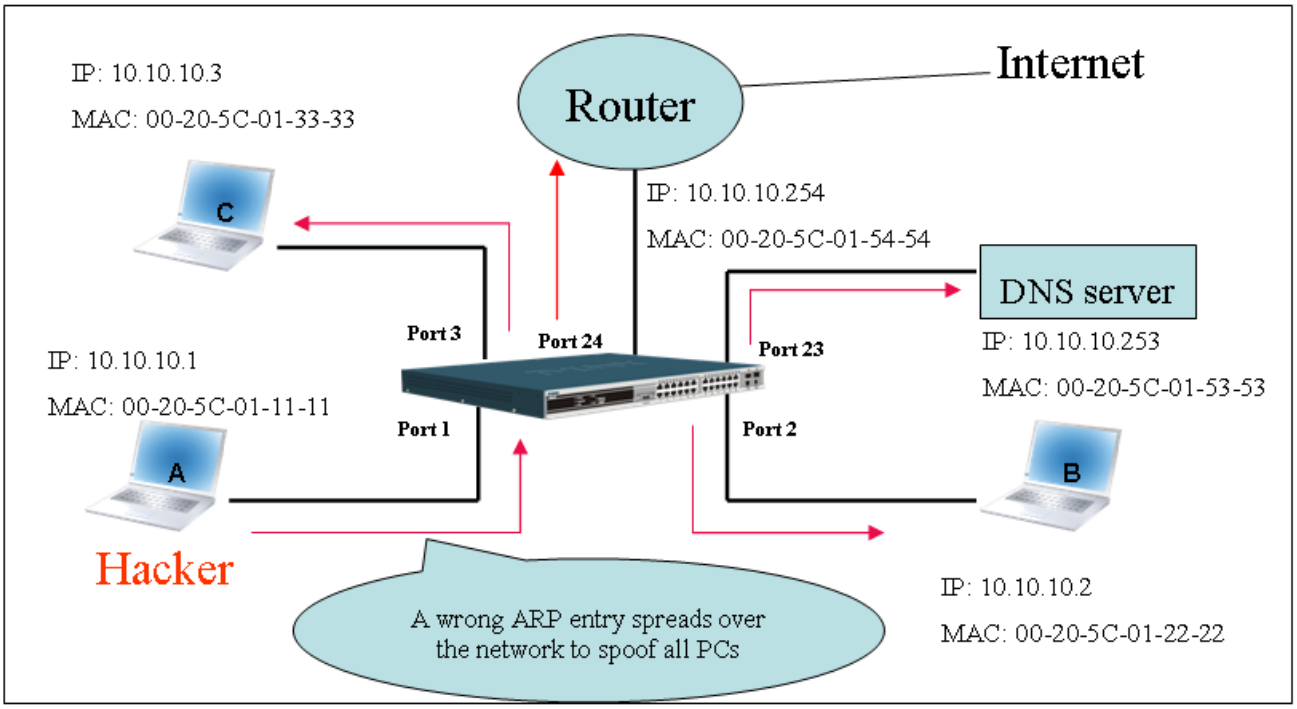


Figure – 4

In the Gratuitous ARP packet, the “Sender protocol address” and “Target protocol address” are filled with the same source IP address. The “Sender H/W Address” and “Target H/W address” are filled with the same source MAC address. The destination MAC address is the Ethernet broadcast address (FF-FF-FF-FF-FF-FF). All nodes within the network will immediately update their own ARP table in accordance with the sender’s MAC and IP address. The format of Gratuitous ARP is shown in Table-5.

Ethernet Header			Gratuitous ARP								
Destination address	Source address	Ethernet type	H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
FF-FF-FF-FF-FF-FF	00-20-5C-01-11-11	0806					**ARP relay**	***00-20-5C-01-11-11***	***10.10.10.254***	***00-20-5C-01-11-11***	***10.10.10.254***

Table – 5

A common DoS attack today can be done by associating a nonexistent or specified MAC address to the IP address of the network's default gateway. The malicious attacker only needs to broadcast one Gratuitous ARP to the network claiming it is the gateway so that the whole network operation will be turned down as all packets to the Internet will be directed to the wrong node.

Likewise, the attacker can either choose to forward the traffic to the actual default gateway (passive sniffing) or modify the data before forwarding it (man-in-the-middle attack). The hacker cheats the victim's PC to think that it is a router and cheats the router to think it is the victim. As can be seen in Figure-5 all traffic will be then sniffed by the hacker but the users will not notice anything happening.

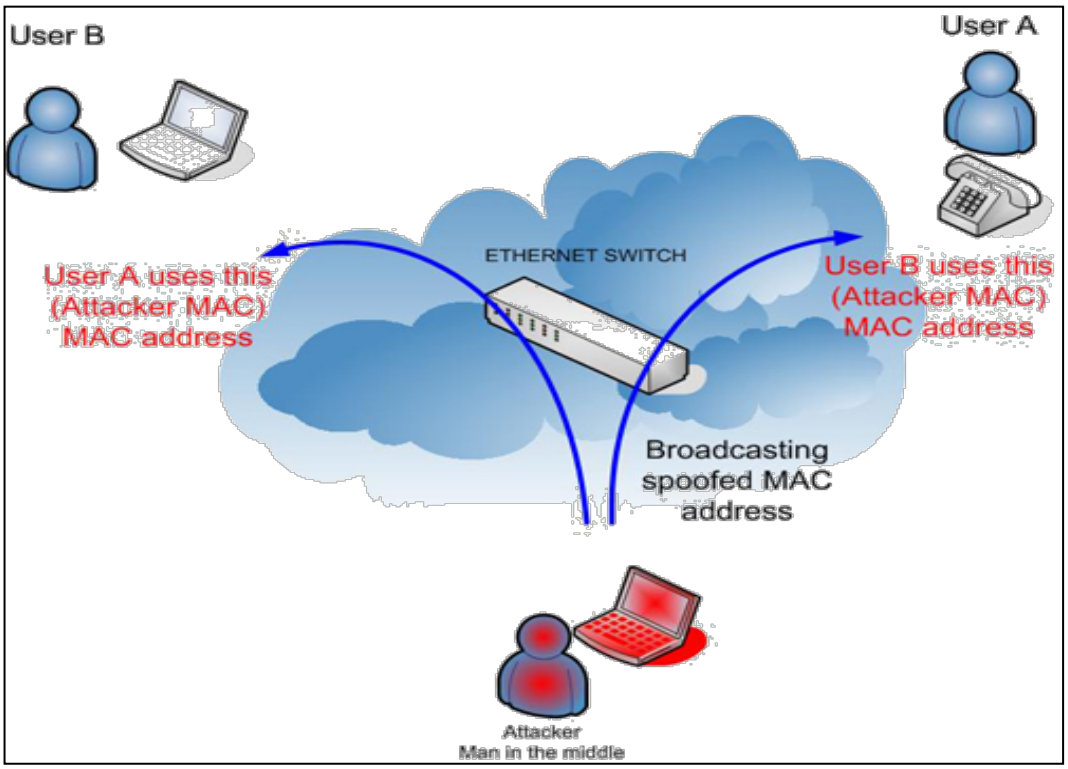
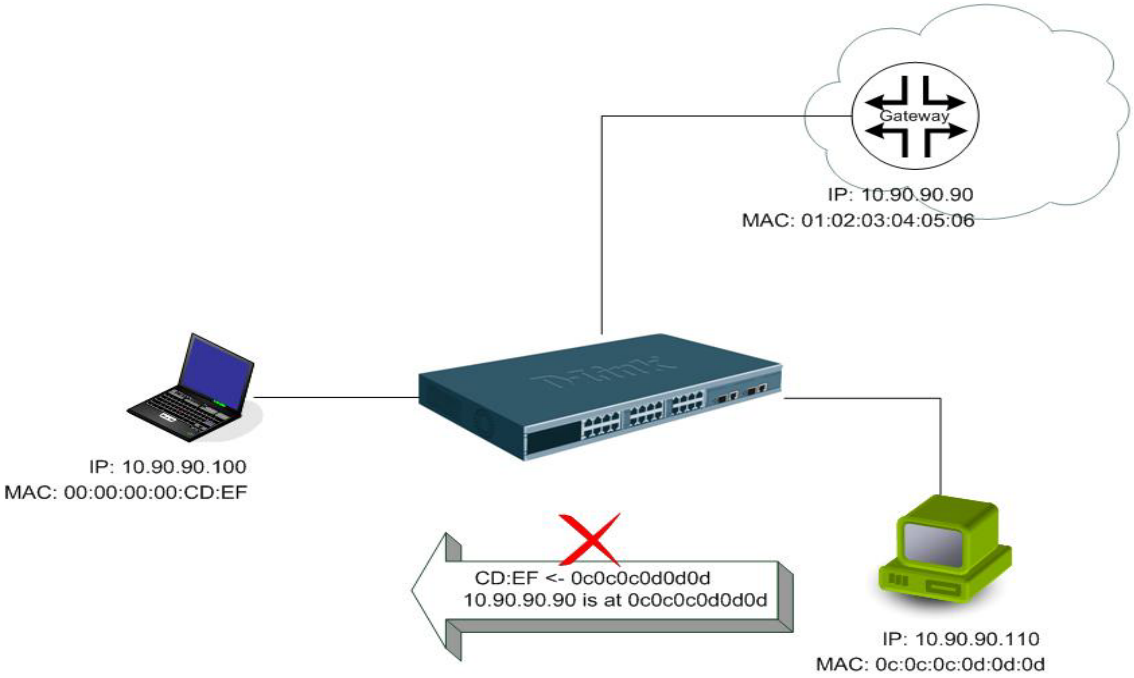


Figure – 5

- ***Prevent ARP spoofing via packet content ACL***

Concerning the common DoS attack today caused by the ARP spoofing, D-Link managed switch can effectively mitigate it via its unique Packet Content ACL.

For that reason the basic ACL can only filter ARP packets based on packet type, VLAN ID, Source and Destination MAC information, there is a need for further inspections of ARP packets. To prevent ARP spoofing attack, we will demonstrate here using Packet Content ACL on DGS-3700 Series to block the invalid ARP packets which contain fake gateway's MAC and IP binding.



Example topology

Configuration:

The configuration logic is listed below:

1. Only when the ARP matches the Source MAC address in Ethernet, the Sender MAC address and Sender IP address in the ARP protocol can pass through the switch. (In this example, it is the gateway's ARP.)
2. The switch will deny all other ARP packets which claim they are from the gateway's IP.

The design of Packet Content ACL on DGS-3700 Series enables users to inspect any offset_chunk. An offset_chunk is a 4-byte block in a HEX format which is utilized to match the individual field in an Ethernet frame. Each profile is allowed to contain up to a maximum of 4 offset_chunks. Furthermore, only one single profile of Packet Content ACL can be supported per switch. In other words, up to 16 bytes of total offset_chunks can be applied to each profile and a switch. Therefore, careful consideration is needed for planning the configuration of the valuable offset_chunks.

In Table-6, you will notice that the Offset_Chunk0 starts from 127th and ends at the second byte. It can also be found that the offset_chunk is scratched from 1 but not zero.

Offset Chunk	Offset Chunk0	Offset Chunk1	Offset Chunk2	Offset Chunk3	Offset Chunk4	Offset Chunk5	Offset Chunk6	Offset Chunk7	Offset Chunk8	Offset Chunk9	Offset Chunk10	Offset Chunk11	Offset Chunk12	Offset Chunk13	Offset Chunk14	Offset Chunk15
Byte	127	3	7	11	15	19	23	27	31	35	39	43	47	51	55	59
Byte	128	4	8	12	16	20	24	28	32	36	40	44	48	52	56	60
Byte	1	5	9	13	17	21	25	29	33	37	41	45	49	53	57	61
Byte	2	6	10	14	18	22	26	30	34	38	42	46	50	54	58	62

Offset Chunk	Offset Chunk16	Offset Chunk17	Offset Chunk18	Offset Chunk19	Offset Chunk20	Offset Chunk21	Offset Chunk22	Offset Chunk23	Offset Chunk24	Offset Chunk25	Offset Chunk26	Offset Chunk27	Offset Chunk28	Offset Chunk29	Offset Chunk130	Offset Chunk31
Byte	63	67	71	75	79	83	87	91	95	99	103	107	111	115	119	123
Byte	64	68	72	76	80	84	88	92	96	100	104	108	112	116	120	124
Byte	65	69	73	77	81	85	89	93	97	101	105	109	113	117	121	125
Byte	66	70	74	78	82	86	90	94	98	102	106	110	114	118	122	126

Table – 6: Chunk and Packet offset indicates a completed ARP packet contained in the Ethernet frame, which is the pattern for the calculation of packet offset.

Ethernet Header			**ARP**								
Destination address	Source address	Ethernet type	H/W type	Protocol type	H/W address length	Protocol address length	Operation	Sender H/W address	Sender protocol address	Target H/W address	Target protocol address
(6-byte)	(6-byte)	(2-byte)	(2-byte)	(2-byte)	(1-byte)	(1-byte)	(2-byte)	(6-byte)	(4-byte)	(6-byte)	(4-byte)
	01 02 03 04 05 06	0806							0a5a5a5a (10.90.90.90)		

Table – 7: A completed ARP packet contained in Ethernet frame

	Command	Description
Step1	create access_profile profile_id 1 profile_name 1 ethernet source_mac FF-FF-FF-FF-FF-FF ethernet_type	- Create access profile 1 To match Ethernet Type and Source MAC address.
Step2	config access_profile profile_id 1 add access_id 1 ethernet source_mac 01-02-03-04-05-06 ethernet_type 0x806 port 1-12 permit	- Configure access profile 1 - Only if the gateway's ARP packet that contains the correct Source MAC in the Ethernet frame can pass through the switch.
Step3	create access_profile profile_id 2 profile_name 2 packet_content_mask offset_chunk_1 3 0x0000FFFF Ethernet Type (2-byte) offset_chunk_2 7 0x0000FFFF SdrIP (First 2-byte) offset_chunk_3 8 0xFFFF0000 SdrIP (Last 2-byte)	- Create access profile 2 - The first Chunk starts from Chunk 3: mask for Ethernet Type (Blue in Table-6:13th &14th bytes) - The second Chunk starts from Chunk 7: mask for Sender IP (First 2-byte) in ARP packet (Green in Table-6: 29th & 30th bytes) - The third Chunk starts from Chunk 8: mask for Sender IP (Last 2-byte) in ARP packet (Brown in Table-6: 31st & 32nd bytes)
Step4	config access_profile profile_id 2 add access_id 1 packet_content offset_chunk_1 0x00000806 Ethernet Type (2-byte):ARP offset_chunk_2 0x00000A5A SdrIP (First 2-byte): 10.90 offset_chunk_3 0x5A5A0000 SdrIP(Last 2-byte): 90.90 port 1-12 deny	- Configure access profile 2 - The rest of the ARP packets whose Sender IP claim they are the gateway's IP will be dropped.
Step5	Save	- Save config

Appendix B

PASSWORD RECOVERY PROCEEDURE

This section describes the procedure for resetting passwords on D-Link Switches.

Authenticating any user who tries to access networks is necessary and important. The basic authentication method used to accept qualified users is through a local login, utilizing a Username and Password. Sometimes, passwords get forgotten or destroyed, so network administrators need to reset these passwords. This section will explain how the Password Recovery feature can help network administrators reach this goal.

The following steps explain how to use the Password Recovery feature on D-Link devices to easily recover passwords.

Complete these steps to reset the password:

1. For security reasons, the Password Recovery feature requires the user to physically access the device. Therefore this feature is only applicable when there is a direct connection to the console port of the device. It is necessary for the user needs to attach a terminal or PC with terminal emulation to the console port of the switch.
2. Power on the switch. After the runtime image is loaded to 100%, the Switch will allow 2 seconds for the user to press the hotkey [^] (Shift + 6) to enter the "Password Recovery Mode". Once the Switch enters the "Password Recovery Mode", all ports on the Switch will be disabled.

```
Boot Procedure                                                  V1.00.B06
-------------------------------------------------------------------------

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

  MAC Address   : 00-19-5B-EC-32-15
  H/W Version   : A1

  Please wait, loading V1.00.B035 Runtime image.............  00 %

The switch is now entering Password Recovery Mode:_
```

```
The switch is currently in Password Recovery Mode.
>
```

3. In the "Password Recovery Mode" only the following commands can be used.

Command	Parameters
reset config	This command resets the whole configuration will be back to the default value
reboot	This command exits the Reset Password Recovery Mode and restarts the switch. A confirmation message will be displayed to allow the user to save the current settings.
reset account	This command deletes all the previously created accounts.
reset password {<username>}	This command resets the password of the specified user. If a username is not specified, the password of all users will be reset.
show account	This command displays all previously created accounts.